OPENTRUST
Securing your business is our signature

Protect and Sign Personal Signature via DocuSign

Certificate Policy

OID: 1.3.6.1.4.1.22234.2.8.3.12

Emmanuel Montacutelli

30/06/2014

DMS_Protect and Sign Personal Signature via DS 1.0

OPENTRUST - Commercial brand of KEYNECTIS
Headquarter: 11-13 rue René Jacques - 92 131 Issy-les-Moulineaux Cedex – France
Tel. : + 33(0)1 55 64 22 00
Fax : + 33(0)1 55 64 22 01

PROTECT AND SIGN PERSONAL SIGNATURE VIA DOCUSIGN

Version	1.0	**Pages**	74
Status	☐ Draft	☒ Final	
Author	Emmanuel Montacutelli	OpenTrust	

Diffusion List	☒ External	☒ Internal
	Public	

History				
Date	Version	Author	Comments	Verified by
30/06/2014	1.0	EM	Creation of the version 1.0	JYF

CONTENT

1 TITRE

1.1 Overview

This Certificate Policy (CP) defines the requirements applicable to the life cycle management of Subscriber (digital) certificates delivered by Protect and Sign (Personal signature) via DocuSign. These Subscriber certificates are aimed at signing electronic documents using OpenTrust and DocuSign trusted services as described in the Protect and Sign (Personal signature) via DocuSign Signature and Proof Management Policy [SPMP].

Subscriber certificates are signed by Subordinate Certification Authorities (Sub-CA) owned by OPENTRUST (according to [SPMP]).

For the purposes of the Protect and Sign (Personal signature) via DocuSign service, the PKI has set up a trust domain that consists of:

- A Root Certification Authority (RCA, also named “Root CA”): used as the trust anchor, that signs intermediate CA certificates and associated Authority Revocation Lists (ARLs). For this PKI, RCA is managed by Adobe and named “Adobe Root CA”.

- An Intermediate CA (ICA): used to sign sub-CA certificates and associated Authority Revocation Lists (ARLs). For this PKI, the ICA is managed by OPENTRUST and named “KEYNECTIS CDS CA”.

- A Subordinate CA (Sub-CA), used to sign Subscriber certificates and CRLs. For this PKI, of the Sub-CAis named “KEYNECTIS K.Websign CDS”.

This CP, that supports the delivery of Subscriber certificates under the Sub-CA, is based on:

- RFC 3647 « Certificate Policy and Certification Practices Framework » issued by the Internet Engineering Task Force (IETF).
- [SPMP]: “Signature and Proof Management Policy, Protect and Sign (Personal Sign) via DocuSign”, version 1.0 minimum.
- [Adobe CP for CDS]: “Adobe Systems Incorporated, CDS Certificate PolicyOctober 2005, Revision #14”.

1.2 Document Name and Identification

Subscriber certificates are issued under OID numbers as given in the table below with the link with the applicable [SPMP]:

PSMP OID	CP OID
1.3.6.1.4.1.22234.2.4.6.1.9	1.3.6.1.4.1.22234.2.8.3.12

1.3 PKI Components

OPENTRUST has established a Policy Management Authority (PMA) to manage the PKI components and services. The PKI is composed of the components described hereafter and supports the following services (PKI services):

- Generation of Sub-CA key pair: generates the sub-CA key pairs and associated CSR during key ceremonies.
- Subscriber registration: consist in collecting and verify Subscriber identity and information that will be used to construct certificate requests and/or included in technical certificates.
- Key pair generation for Subscriber: consist in generate key pair for a Subscriber.
- Subscriber certificate generation: generating Subscriber certificates.
- Log trail generation: generates log that are used either for the audit purpose or to be analyzed in order to solve an incident.

- Publication of a CRL: a CRL is issued by CA for Subscriber certificate. This CRL is always empty because there is no revocation service for Subscriber.
- OCSP services: CA delivers OCSP status information for the Subscriber certificate.
- Publication services: publication of Sub-CA certificate and all relevant information related to the use of Sub-CA services and Subscriber certificate.

This CP gives the security requirements applicable to all services while the associated Certification Practice Statement (CPS) will give more details on practices enforced by each components participating in the PKI activities.

1.3.1 Policy Management Authority (PMA)

The PMA is the PKI lead authority and is managed by OPENTRUST.

The PMA approves CP and Certification Practice Statement (CPS) used to support the PKI certification services.

The PMA defines the organization of PKI components and services, is in charge of nominating the PKI components and verifying the compliance of the services they deliver with applicable sections of this CP and its corresponding CPS.

PMA main mission at minimum the following:

- Approves PKI services and prices to be delivered by the PKI infrastructure.
- Approves Certificate Policies.
- Approves CA creation and revocation.
- Approves the choice of RCA and ICA used to sign Sub-CA.
- Approves cryptographic specification (algorithms used for signature, encryption, authentication, hash functions and key length, operational lifetime) for the PKI systems and any related change.
- Approves the specifications of cryptographic tokens that generate keys and host subscribers certificates
- Approves PKI applications standards. This will guarantee the required level of interoperability and acceptance by RCA.
- Approves compliance between security practice documents and related policies (for instance CPS/CP).
- Approves final annual internal audit report of all the PKI's components.
- Approves external audit report of RA performed by OpenTrust.
- Manages external audit of RA.
- Controls procedures defined by Client for Subscriber management.
- Guarantees the validity and the integrity of the PKI published information.
- Ensures that a proper process to manage security incidents within the PKI services and PKI components is in place.
- Arbitrates disputes relating to the PKI services and the use of certificates and ensures that the resolution of such disputes is published.

1.3.2 Subordinate Certification Authorities (Sub-CA)

The Sub-CA is owned by OPENTRUST and operated by OPENTRUST.

The Sub-CA supports the following PKI services:

- Generation of Sub-CA key pairs.
- Subscriber certificate generation.
- Generation and publication of CRLs.
- Log trail generation.

The Sub-CA operates its services according to this CP and the corresponding CPS. The Sub-CA cannot start operation without prior approval of the PMA.

1.3.3 Registration Authority (RA)

The RA is owned by the Client. The RA is operated by an entity designated by the Client.

The Client may rely on:

- Its own IT system to manage Subscriber's information, or
- On DocuSign IT system.

DocuSign performs the Consent Protocol, manages electronic document to be signed, Subscriber's information transmitted by Client and manages communication with the CA. Client and Subscriber don't have direct access to the CA. Client and Subscriber only have access to DocuSign portal.

The RA supports the following PKI services:

- Subscriber registration.
- Log trail generation.

The RA is designated and authorized by the Sub-CA on a contractual basis through a Client contract. Consequently, the Client as a RA documents and implements procedures for the identification of legal entities and private individuals, in accordance with the rules it has defined based on its needs, particularly in the Consent Protocol. Its role is to prove that the requester matches the identity and attributes that will be indicated in the Certificate. These identification procedures vary depending on the level of trust the RA decides to apply to this verification.

The RA is responsible to define procedure that address especially section 3, 4, 5, 6, 8 and 9 of the present CP that concerns the RA. If the Client designates a different legal entity different from the Client, then a contract, or legal document according the link between the Client and legal Entity designated by Client, has to be established between Client and the legal entity designated by the Client in order to cover the RA services addressed by the designated entity.

Procedures to manage Subscribers, defined by the RA, are performed by an RA Operator. The RA is responsible to establish and maintain a list of all RA Operators that are allowed to enroll Subscribers.

An RA operates its services according to this CP and the corresponding CPS. An RA cannot start operation without prior approval of the PMA.

1.3.4 Operational Authority (OA)

The Operational Authority (OA) is the entity that hosts and manages all the software, hardware and HSM used to support PKI services. The OA is the entity which sets up and realizes all operations for the PKI services. The CPS gives details on how each service is provided to each PKI component.

PKI components are operated by:

- OPENTRUST which is the OA for the Sub-CA and Publication Service.
- DocuSign which is the OA for the RA for Service "DocuSign" (refer to [SPMP]).
- Client which is the OA for its software used in RA operations.

OAs operates their services according to this CP and the corresponding CPS. OAs cannot start operation without prior approval of the PMA.

1.3.5 Publication Service (PS)

PS is owned by OPENTRUST and operated by OPENTRUST.

The Publication Service (PS) is the OPENTRUST repository (refer to chapter 2 below) which provides the following PKI services:

- Publication services (refer to section 2 below).
- Log trail generation.

1.3.6 Subscriber

A Subscriber is a physical person whose identity appears as subject in a Subscriber Certificate and who signs a document according rules defined in [SPMP]. Subscriber key pair and certificate generation are linked to the signature operation performed by Subscriber according [SPMP] and Client choice made for Consent Protocol and RA registration policy.

Subscribers abide to this CP and the associated procedures as described in the RA documentation.

1.3.7 Other Participants

1.3.7.1 Client

Client is a Legal Entity that establishes a contract with OPENTRUST or DocuSign to use Protect and Sign (Personal signature) via DocuSign service according [SPMP]. Client designates entity that is RA. In the contract between Client and OPENTRUST or DocuSign all RA obligations are included. Client defines enrollment rules that RA shall implements and selects and defines the Consent Protocol. Consent Protocol may request the use of a technical activation data from Subscriber. RA is audited according rules defined in section 8 below.

1.3.7.2 Relying Parties

Relying Parties are entities that act in reliance on the validity of the binding of the Subscriber identity to a public key. A Relying Party is responsible for deciding how to check the validity of a Subscriber certificate, at least by checking the appropriate certificate status information (using CRLs and ARLs or OCSP responses) for the Subscriber, Sub-CA, ICA and Root CA certificates. A Relying Party may use information in the certificate (such as Certificate Policy identifiers) to determine the suitability of the certificate for a particular use.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Use

1.4.1.1 Sub-CA Certificate

A Sub-CA certificate is used to validate Subscriber certificates and CRLs and OCSP certificate it has delivered.

Each Sub-CA private key is allowed to sign the following types of certificates:

- Sub-CA CSR.
- Subscriber certificate.

1.4.1.2 Subscriber

The uses of private key are the following:

- Used to sign electronic document according Consent Protocol and Client Signature Policy and [SPMP].
- Used to sign CSR (Pkcs#10 format).

The uses of certificate are the following:

- Used to verify electronic signature applied on document using Protect and Sign (Personal signature) service.

Signature created with Subscriber Certificate giving to signed document the same legal value as a paper document, in accordance with article 1316-1 and the first sentence of the second paragraph of article 1316-4 of the French Civil Code and point 1 of Article 2 ("Definitions") of the "DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures".

Client is informed that Subscriber Certificates issued using the PKI services does not meet the definition of "qualified" under article 6 of French decree no. 2001-272 of 30 March 2001 and does not meet the definition of "qualified signature" under Article 5 (Legal effects of electronic signatures, point 1) of the "DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures". As a result, electronic signatures using the Service are not presumed reliable under article 1316-4, paragraph 2, of the French Civil Code and article 2 of the aforementioned decree and under Article 5 (Legal effects of electronic signatures, point 1) of the "DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures".

1.4.2 Prohibited Certificate Use

No other uses than the ones stated in section 1.4.1 above are covered by this CP.

OPENTRUST is not responsible for any other use than the ones stated in this CP.

1.5 Policy Administration

1.5.1 Organization Administering the Document

PMA is responsible for all aspects of this CP and the associated CPS.

1.5.2 Contact Person

The person to contact is:

- Mr. Jean-Yves Faurois.
- Director of Managed Services at OPENTRUST.
- OPENTRUST – 11-13 rue René Jacques - 92131 Issy-les-Moulineaux Cedex – FRANCE
- Phone: (+33) (0)1 53 94 22 00
- Fax: (+33) (0)1 53 94 22 01

1.5.3 Person Determining CPS Suitability for the Policy

The PMA approves the CPS. The PKI will be audited periodically to verify compliance as per PMA guidelines and standards approved by the PMA. The Audit ensures that the CPS is implemented correctly and is compliant with the CP. Further, the PMA reserves the right to audit the PKI as set in section 8 of this CP.

In any case, determination of compliance shall be based on independent audits.

1.5.4 CPS Approval Procedures

Amendments shall either be in the form of a new CPS (with a sum up of the modifications) or an update notice that contains the modifications and the references in the previous CPS. The creation or modification of the existing CPS is at the discretion of the PMA. A new CPS automatically replaces the previous one and becomes operational as soon as the PMA has approved it. Any new CPS or update to the existing CPS must be compliant with this CP before approval.

1.6 Definitions and Acronyms

1.6.1 Definitions

Term	Definition
Accreditation	Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk.
Activation Data	Secret data (e.g.: password, PIN code, certificate or OTP) that is used to perform cryptographic operations using a Private Key.
Audit	An independent review and examination of documentation, records and activities to access the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies or procedures.
Authentication	The process whereby one party has presented an identity and claims to be that identity and the second party confirms that this assertion of identity is true.
Authentication data	Particular technical activation data (like for example OTP or authentication certificate) used by Subscriber to be authenticated by Protect and Sign (Personal signature) service in order to sign a document according a Consent Protocol.
Authority Revocation List (ARL)	A list of revoked Certification Authority Certificates. Technically, an ARL is a CRL.
Availability	The property of being accessible and upon demand by an authorized entity [ISO/IEC 13335-1:2004]. It means that an electronic data stored using means (hard disk, paper …) can be still readable and have the same meaning after and during its storage.

Certificate	A Certificate is a data structure that is digitally signed by a Certification Authority, and that contains the following pieces of information: o The identity of the Certification Authority issuing it. o The identity of the certified Subscriber. o A Public Key that corresponds to a Private Key under the control of the certified Subscriber. o The Operational Period. o A serial number. o The Certificate format is in accordance with ITU-T Recommendation X.509 version 3.
Certificate Extension	A Certificate may include extension fields to convey additional information about the associated Public Key, the Subscriber, the Certificate Issuer, or elements of the certification process.
Certificate Manufacturing	The process of accepting a Public Key and identifying information from an authorized Subscriber, producing a digital Certificate containing that and other pertinent information, and digitally signing the Certificate.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a Certificate to a particular community and/or class of applications with common security requirements.
Certificate Request	A message sent from a Client to a Sub-CA in order to apply for a digital Certificate. The Certificate request contains information identifying the Subscriber and sometimes activation data.
Certificate Revocation List (CRL)	A list of revoked Certificates that is created and signed by a CA. A Certificate is added to the list if revoked (e.g., because of suspected key compromise, distinguished name (DN) change) and then removed from it when it reaches the end of the Certificate's validity period. In some cases, the CA may choose to split a CRL into a series of smaller CRLs. When a Subscriber chooses to accept a Certificate the Relying Party Agreement requires that this Relying Party check that the Certificate is not listed on the most recently issued CRL.
Certificate Validity Period	The certificate validity period is the time interval during which the CA warrants that it will maintain information about the status of the certificate. [RFC 3280].
Certification Path (also called trusted path or trusted certification chain)	A chain of multiple certificates needed to validate a certificate containing the required public key. A certificate chain consists of a RCA-certificate (anchor), CA-certificate and the Subscriber certificates signed by the CA.

Certification Practice Statement (CPS)	A statement of the practices, which a CA employs in issuing and revoking Certificates, and providing access to same. The CPS defines the equipment and procedures the CA uses to satisfy the requirements specified in the CP that are supported by it.
Client Contract	Document(s) signed by Client to legally binding Client as RA to OpenTrust and to OpenTrust or DocuSign for the use of Service (depending if the Client is a client of OpenTrust or DocuSign) as defined in [SPMP].
Common Criteria	Common Criteria for Information Technology Security Evaluation is an international standard (ISO/IEC 15408) for information technology security certification.
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information may have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key.
Confidentiality	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes [ISO/IEC 13335-1:2004].
Cryptographic domain (for HSM)	Trusted environment that contains one or several keys and managed with dedicated activation data. This trusted environment is deployed in a Hardware Security Module (HSM) to activate and use keys.
Consent Protocol	Means the procedure according to which DocuSign collects the consent of the Subscriber to: – Receive a Certificate under the Subscriber Certificate Personal Identity. – Accept to sign the Electronic Document. – Accept General Terms of Use The Consent Protocol is executed between DocuSign and the Subscriber.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a person who has received a digitally signed message can determine: • Whether the transformation was created using the private signing key that corresponds to the signer's public verification key. • Whether the message has been altered since the transformation was made.
Directory	A directory system that conforms to the ITU-T X.500 series of Recommendations.

Disaster Recovery Plan	A plan defined by a CA to recover its all or part of PKI services, after they've been destroyed following a disaster, in a delay define in the CP/CPS.
Distinguished Name	A string created during the certification process and included in the Certificate that uniquely identifies the Subscriber within the CA domain.
Encryption Key Pair	A public and private Key Pair issued for the purposes of encrypting and decrypting data.
Federal Information Processing Standards (FIPS)	Federal standards that prescribe specific performance requirements, practices, formats, communications protocols, etc. for hardware, software, data, telecommunications operation, etc. U.S. Federal agencies are expected to apply these standards as specified unless a waiver has been granted in accordance with agency waiver procedures.
Hardware Security Module (HSM)	An HSM is a hardware device used to generate cryptographic Key Pairs, keep the Private Key secure and generate digital signatures. It is used to secure the CA keys, and in some cases the keys of some applications (Subscribers).
Hash Function	A function which maps string of bits to fixed-length strings of bits, satisfying the following two properties: - It is computationally infeasible to find for a given output an input which maps to this output; - It is computationally infeasible to find for a given input a second input which maps to the same output [ISO/IEC 10118-1].
Internet Engineering Task Force(IETF)	The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researches concerned with the evolution of the Internet architecture and the smooth operation of the Internet.
Integrity	Refers to the correctness of information, of originator of the information, and the functioning of the system which processes it.
Interoperability	Implies that equipment and procedures in use by two or more entities are compatible, and hence that it is possible to undertake common or related activities.
Key Ceremony (KC)	A Key Ceremony (KC) is an operation enabling the management (generation and destruction) of cryptographic key pairs and CA life-cycle (certificate signature and revocation). A key ceremony requires a minimum number of trusted employees whom represent the owner of the PKI.
Key Generation	The process of creating a Private Key and Public Key pair.
Object Identifier (OID)	An object identifier is a specially-formatted sequence of numbers that is

	registered with an internationally-recognized standards organization.
OCSP	Protocol useful in determining the current status of a digital Certificate without requiring CRLs.
Operational Period of a Certificate	The operational period of a Certificate is the period of its validity. It would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and end on the date and time it expires as noted in the Certificate or earlier if revoked.
Organization	Department, agency, partnership, trust, joint venture or other association.
PIN	Personal Identification Number. See activation data for definition
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request.
PKI Disclosure Statement (PDS)	Defined by IETF's RFC 3647 as "An instrument that supplements a CP or CPS by disclosing critical information about the policies and practices of a CA/PKI. A PDS is a vehicle for disclosing and emphasizing information normally covered in detail by associated CP and/or CPS documents. Consequently, a PDS is not intended to replace a CP or CPS.
PKIX	IETF Working Group chartered to develop technical specifications for PKI components based on X.509 Version 3 Certificates.
Private Key	The Private Key of a Key Pair used to perform Public Key cryptography. This key must be kept secret.
Public Key	The Public Key of a Key Pair used to perform Public Key cryptography. The Public Key is made freely available to anyone who requires it. The Public Key is usually provided via a Certificate issued by a Certification Authority and is often obtained by accessing a repository.
Public Key Infrastructure (PKI)	A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private Key Pairs, including the ability to issue, maintain, and revoke Public Key Certificates.
Public/Private Key Pair (also named Key Pair)	Two mathematically related keys, having the properties that (i) one key can be used to encrypt data that can only be decrypted using the other key, and (ii) knowing one of the keys which is called the Public Key, it is computationally infeasible to discover the other key which is called the Private Key.
Sub-CA domain space	Sub-CA domain space is the set of all the certificates delivered by the Sub-CA.

Registration	The process whereby a user applies to a Certification Authority for a digital Certificate.
Repository	Publication service providing all information necessary to ensure the intended operation of issued digital Certificates (e.g.: CRLs, encryption Certificates, CA Certificates).
Revocation	To prematurely end the Operational Period of a Certificate from a specified time forward.
RFC3647	Document published by the IETF, which presents a framework to assist the writers of Certificate Policies or certification practice statements for participants within Public Key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on Certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a Certificate Policy or a certification practice statement.
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman.
Signature Key Pair	A public and private Key Pair used for the purposes of digitally signing electronic documents and verifying digital signatures.
Trusted Role	Those individuals who perform a security role that is critical to the operation or integrity of this PKI.
Trustworthy System	Computer hardware, software, and/or procedures that: (a) are reasonably secure from intrusion and misuse; (b) provide a reasonable level of availability, reliability, and correct operation; (c) are reasonably suited to performing their intended functions, and (d) adhere to generally accepted security procedures.
Valid Certificate	A Certificate that (1) a Certification Authority has issued, (2) the Subscriber listed in it has accepted, (3) has not expired, and (4) has not been revoked. Thus, a Certificate is not “valid” until it is both issued by a CA and has been accepted by the Subscriber.

1.6.2 Acronyms

Acronym	Means
AES	Advanced Encryption Standard
ARL	Authority Revocation List
CA	Certification Authority

CDS	Adobe Certified Document Services
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certification Revocation List
CSR	Certificate Signing Request
DES	Data Encryption Standard
DN	Distinguished Name
EAL	Evaluation assurance level, ISO 15408 (Common Criteria) norm for certification of security products
FIPS	United States of America, Federal Information Processing Standards
HTTP	Hypertext Transport Protocol
IP	Internet Protocol
ISO	International Organization for Standardization
LDAP	Lightweight Directory Access Protocol
MBUN	“Meaningless But Unique Number” a number that is assigned by the PKI to assist in differentiating Subscribers with otherwise similar attributes.
MofN	M out of N (Threshold Scheme)
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
PIN	Personal Identification Number
PKCS	Public-Key Cryptography Standard
PKI	Public Key Infrastructure
PS	Publication Service

RCA	Root Certification Authority
RFC	Request For Comment
RSA	Rivest, Shamir, Adleman
SHA	Secure Hash Algorithm
SSL	Secure Socket Layer
Sub-CA	Subordinate CA
TDES	Triple DES
TLS	Transport Layer Security

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Publication Service is responsible for making available the any published information related to the Sub-CA services.

The PS shall be deployed so as to provide high levels of reliability (24 out of 24 hours, 7 out of 7 days)

2.2 Publication of Certification Information

The PS publishes the following data:

- CP: http://www.OpenTrust.com/
- OPENTRUST Sub-CA certificate: http://www.OpenTrust.com/
- CRL: http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_KWebsign_CDS.

CA ensures that terms and conditions are made available to Subscribers and Relying Party as following:

- Subscriber: CA's terms and conditions are shown to the Subscriber during the Consent Protocol and accepted by Subscriber during the Consent Protocol.
- Relying Party: terms and conditions and information as required to be published for Relying party are already contained in the present CP in sections; 1.4, 4.5.2, 5.5, 9, 9.6, 9.7, and 9.8.
- Client is responsible to establish and make available particular terms and conditions about signature process and personal data maangement for Relying Party and Subscriber.
- DocuSign: DocuSIgn's terms and conditions for the use of DocuSign's Service "DocuSign" (refer to [SPMP]) are made available to Client and Subscriber by DocuSign.

2.3 Time or Frequency of Publication

The information identified in section 2.2 above are made available:

- CP:
  - Before start of service for the initial CP.
  - No later than 48 hours after any CP update or replacement is approved by the PMA.
- Sub-CA certificate:
  - Before start of service for the initial Sub-CA and no later than 48 hours after generation of Sub-CA certificates following a renewal or re-key.

2.4 Access Controls on Repositories

The PS is responsible for the security policy set granting access to the published information.

Access to read information is publicly and internationally available through the Internet, in readily language, for the following information for CP and Sub-CA certificate.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

The attribute fields for “Issuer Name” and “Subject” shall be compliant with RFC 5280. Details for the type of use coding are given below.

3.1.1.1 Sub-CA

The DN content for Sub-CA certificates is detailed in section 10 below.

3.1.1.2 Subscriber

The DN content for Subscriber certificates is detailed in section 10 below.

3.1.2 Need for Names to Be Meaningful

The certificates issued pursuant to this CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person to which they are assigned in a meaningful way and shall be in line with the identity card of the Subscriber

3.1.2.1 Sub-CA

A key pair can be linked with only a unique CN for each Sub-CA certificate.

3.1.2.2 Subscriber

The RA is sole responsible for defining the Subscriber identity to be set in the Subscriber certificate.

3.1.3 Anonymity or Pseudonymity of Certificate

This policy does not permit anonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

3.1.4.1 Sub-CA

Relying parties shall use the subject name contained in the certificate (refer to section 3.1.1) to identify the Sub-CA.

3.1.4.2 Subscriber

Subscriber certificates can be identified using the CN field contained in the DN. The CN field is not guaranteed to be unique.

3.1.5 Uniqueness of Names

3.1.5.1 Sub-CA

Names contained in any Sub-CA certificate (refer to section 3.1.1 above) shall be unique in the ICA trust domain, and all names shall be provided to the entity providing ICA services for inclusion in the appropriate name constraint values of the Sub-CA Certificate.

3.1.5.2 Subscriber

A certificate's uniqueness is based on the uniqueness of its serial number within the domain of the CA.

The RA shall be responsible for ensuring DN uniqueness in Certificates issued by the Sub-CA, and for handling DN-related conflicts. To do so, the RA must create a unique TransNUM (Transaction identifier) for each Subscriber and signed document to be inserted by CA in the DN of Subscriber Certificate.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulations.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

3.2.1.1 Sub-CA

Sub-CA key pairs shall be generated, stored, activated, used, and destroyed by the OA in a way that demonstrates to the PMA that each Sub-CA owns the private key corresponding to the public key contained in its Sub-CA certificate.

3.2.1.2 Subscriber

For Subscriber Certificates, proof of ownership of the private key corresponding to the Subscriber Certificate used for signing purposes is provided by the technical and organizational resources defined in the Consent Protocol, chosen by Client, used and applied as part of the Protect and Sign (Personal signature) Service when the certificate request is made.

3.2.2 Authentication of Organization Identity

3.2.2.1 Subscriber

Where the Subscriber is a person who is identifier in association with a Legal person, or other organizational entity, evidence shall be provided, and verified by RA, of:

- Full name and legal status of the associated legal person or other organizational entity.
- Any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- Evidence that the subject is associated with legal person or other organizational entity.

RA can use internal or external (like DUNS, official government data source…) data source to proceed to verification.

3.2.3 Authentication of Physical Person Identity

3.2.3.1 Subscriber

The RA is also responsible for collecting and storing the required information in order to provide evidence of the Subscriber identity set in the certificate.

The enrollment of a User prior to issuing a Subscriber Certificate is performed directly by the RA.

Subscriber identity verification rules are left to the discretion of the RA, which is in charge of managing the Subscriber.

The procedure for identifying, authenticating and validating a request to issue a certificate is described in the Proof Management Policy and in the Consent Protocol used for each Client using Subscriber Certificates, and is supplemented by a procedure specific to the RA's line of business defined by the Client.

The method of assigning this identity is therefore defined by the Client, which enrolls all of its Users with its identification data.

RA shall collect either direct evidence, or an attestation from an appropriate and authorized source, of the identity (e.g. surname and given names consistent with the applicable law and national identification practices) and, if applicable, any specific attributes of subscriber to whom a certificate is issued. Submitted evidence may be in the form of either paper or electronic documentation. Verification of the Subscriber's identity shall be at time of registration by appropriate means and in accordance with national law.

RA can use internal or external data source to proceed to verification.

3.2.4 Validation of Authority

The authentication and identification of an authority of a subscriber's is done by the RA using and verifying information required by section 3.2.2 above.

Any Certificates issued by any CA that contain explicit or implicit Subscriber entity affiliation shall be issued only pursuant to the stipulations of section 3.2.2 above.

3.2.5 Non-Verified Subscriber Information

There is no non verified information used by the RA to fill a certificate.

3.2.6 Criteria for Interoperation

Certificates delivered by PKI components are managed according to the rules and requirements stated by the CA and Client and Adobe CPS.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

3.3.1.1 Sub-CA

Same procedures as described in section 3.2 above apply.

3.3.1.2 Subscriber

For this section, Subscriber is already registered by RA and has been successfully issued a first certificate. Then RA can define a process to issue again others Certificates for the Subscriber. But in this case, as major and most important information used initially to register Subscriber may stayed valid, RA may want to avoid to register again completely the subscriber as in section 3.2 above.

The RA is also responsible for updating, collecting and storing the required information in order to provide evidence of the Subscriber identity set in the certificate during renewal operation.

The enrollment for renewal of a User prior to issuing a Subscriber Certificate is performed directly by the RA.

Subscriber identity verification rules are left to the discretion of the RA, which is in charge of managing the Subscriber for renewal operation.

The procedure for identifying, authenticating and validating a request to issue a new certificate is described in the Proof Management Policy and in the Consent Protocol used for each Client using Subscriber Certificates, and is supplemented by a procedure specific to the RA's line of business defined by the Client.

The method of assigning this identity for a new certificate is therefore defined by the Client, which enrolls all of its Users with its identification data and authentication data.

If any of the CA terms and conditions have changed, these shall be communicated to the Subscriber and Subscriber shall sign the new terms and condition (refer to section 4.1.2 below).

If any information of Subscriber to be set in Subscriber certificate (refer to section 3.1.1 above) have changed then the registration shall be performed against procedure as defined in section 3.2 above at least concerning information that have changed.

Information used to authenticate Subscriber during consent protocol (like email address and phone number) can only be modified by Subscriber after verification performed by RA in order to be sure that update information are linked to the Subscriber for consent protocol.

3.3.2 Identification and Authentication for Re-key After Revocation

3.3.2.1 RCA, ICA and CA

Same procedures as described in section 3.2 above apply.

3.3.2.2 Subscriber

Same procedures as described in section 3.2 above apply.

RA shall document its rules for re-key for depending on the type of revocation causes.

3.4 Identification and Authentication for Revocation Request

3.4.1.1 Sub-CA

Sub-CA revocation requests shall only be authorized by PMA members.

3.4.1.2 Subscriber

Not applicable.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Sections 4.1, 4.2, 4.3 and 4.4 specify the requirements for an initial application for certificate issuance. Sections 4.6, 4.7 and 4.8 specify the requirements for certificate renewal.

4.1.1 Who Can Submit a Certificate Application

4.1.1.1 Sub-CA

The authorized representative of the Sub-CA shall submit the certificate request as directed by the PMA.

4.1.1.2 Subscriber

Certificate request is under responsibility of RA.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 Sub-CA

Sub-CA certificates must be authorized by the PMA prior to issuance. The issuance process will include documenting the following information:

- Identity to set in the certificate (refer to section 3.1.1 above).
- Legal Entity identification data, i.e. full name and legal status of the associated legal person or other organizational entity and any relevant existing registration information (e.g. company registration) of the associated legal person or other organizational entity.
- CSR associated with the generated key pair (refer to section 6.1.1). The CSR shall be included in the application.
- Authorized representative information:
    - The full name, including surname and given name(s) of the representative.
    - The full name and legal status of the authorized representative's Employer.
    - A place of business physical address or other suitable method of contact for the authorized representative.

4.1.2.2 Subscriber

Certificate request shall contain sufficient information in order to give proof of Subscriber's claimed identity to be set in Subscriber certificate. At least the Subscriber shall provide or RA shall collect and verify:

- Subscriber's a physical address, or other attributes (email or phone number), which describe how the subscriber may be contacted.

- Subscriber's full name (included surname and given names consistent with the applicable law and national identification practices).

- If the Subscriber is a person who is identifier in association with a Legal person, or other organizational entity, evidence shall be provided of information requested in section 3.2.2 above.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 Sub-CA

Requests are submitted by an authorized representative at the discretion of the PMA prior to issuance. It is the responsibility of the PMA to authenticate the authorized representative as described in section 3.2 above, and to verify that the information in Certificate request is accurate for the CA.

4.2.1.2 Subscriber

It is the responsibility of the RA to verify that the information in Certificate request is accurate for a Physical person (refer to sections 3.2.2 and 3.2.5 above). RA shall document the verification process in its Registration policy.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 Sub-CA

The PMA shall be responsible for approving or rejecting the Sub-CA certificate applications.

4.2.2.2 Subscriber

The RA shall be responsible for approving or rejecting Subscriber certificate applications.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

4.3.1.1 Sub-CA

The PMA shall transmit the certificate request to the OA and Root CA. The OA shall authenticate the certificate request prior to the generation of the Sub-CA key pair and CSR. Transmission of the certificate request and CSR shall be performed in a manner which ensures the integrity of the information.

The following actions must occur during a Sub-CA Key Ceremony, which shall be witnessed by an OPENTRUST PMA witness:

- Issuance of Sub-CA keys.
- Backup of Sub-CA private key.
- Generation of Sub-CA CSR (The CSR shall include the Sub-CA's public key).
- Generation of Sub-CA certificate.

4.3.1.2 Subscriber

Subscriber uses the activation data, if Client chosen to use activation data (not mandatory), in RA interface (Service "DocuSign") according the Consent Protocol chosen by Client. Consent Protocol may require a technical activation data (for example: OTP code).

RA authenticates the Subscriber using the activation data and transmits technical certificate request to CA (refer to section 6.2.8.2 below).

Subscriber's key pair are generated (refer to section 6.1.1.2 below) by Protect and Sign (Personal Signature) platform. CSR is transmitted to CA (refer to section 6.1.3 below).

CA generates the Subscriber certificate.

Protect and Sign (Personal signature) service (Service "PSM" as described in [SPMP]) signs and time stamps the fingerprint of the document transmitted by RA.

After signature of the fingerprint of the document, Subscriber key pair is destroyed.

CA transmitted the signed and time stamped fingerprint to the RA

RA (Service "DocuSign") includes Subscriber certificate, contained in the signed and time stamped fingerprint value generated by OpenTrust, inside the document.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Not applicable

4.4 Certificate Acceptance

4.4.1 Conducting Certificate Acceptance

4.4.1.1 Sub-CA

Acceptance of the Sub-CA certificate shall be performed by the PMA. The Sub-CA shall neither issue certificates nor sign CRLs until the Sub-CA certificate has been accepted.

4.4.1.2 Subscriber

If there is a mistake in the Subscriber certificate, then RA shall be alerted by the person (RA or Subscriber) who performs the verification.

4.4.2 Publication of the Certificate by the PS

Subscriber Certificate is contained in the signed document. Therefore Client shall make available the signed document in order to make available the certificate.

For Relying Party, the Subscriber certificate of a particular Subscriber is also contained in the associated signed document and therefore will be available to a Relying Party if the Relying Party has the signed document.

Relying party can test the certificate using information published by CA (refer to section 2.2 above).

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Client and RA are notified of certificate issuance by CA according Protect and Sign (Personal signature) services.

4.5 Key Pair and Certificate Usage

4.5.1 Private Key and Certificate Usage

Subscribers and the Sub-CA shall use their Private Keys for the purposes set forth in section 1.4 above. Usage of a key pair and the associated certificate shall also be performed as indicated in the certificate itself, via extensions related to key pair usage (refer to section 6.1.7 below).

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties use the trusted certification path and associated public keys for the purposes constrained by the certificates extensions (such as key usage, extended key usage, certificate policies, etc.) and to authenticate the trusted common identity of Subscriber certificates.

Relying parties has to be aware of the security rules to be deployed in the Client electronic transaction for the usage of a Subscriber certificate. A Subscriber certificate is used to identify, for example, Subscriber as a physical person who sometimes belongs to an External Entity. Relying party has to check additional information (key usage, OID policy ...) in order to accept and use the right Subscriber certificate in the electronic transaction. The relying party has to use all the required information in the certificate (DN as described in section 3.1.1 above, extensions ...) in order to be sure to accept the right Subscriber.

A Subscriber certificate can't be used without preliminary check from Relying party like for example trusted path, additional information only known from Subscriber and Relying party (in order to register the Subscriber's certificate) and Client information about Subscriber enrollment and use of signed document verifiable using Subscriber certificate.

4.6 Certificate Renewal

According to RFC 3647, certificate renewal is a process in which only the validity period and the serial number of the certificate are changed (neither the public key nor any other information in the certificate are changed).

This practice is not allowed for Sub-CA and Subscriber certificates. If a new certificate is created, a new key pair is created.

4.7 Certificate Re-key

Certificate re-key shall be processed when a key pair reaches the end of its life (refer to section 6.3.2 below), the end of operational use, or when the public key is compromised. A new key pair shall be generated in all cases.

4.7.1 Sub-CA

The same procedures as those applied for initial generation shall apply for a new Sub-CA certificate and associated key pair generation (refer to sections 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.2.3**Erreur ! Source du renvoi introuvable.**, 4.3.1, 4.4.1 and 4.4.2 above).

4.7.2 Subscriber

Refer to section 4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.2.3**Erreur ! Source du renvoi introuvable.**, 4.3.1, 4.4.1 and 4.4.2 above but for authentication it is the section 3.3 that shall be applied.

4.8 Certificate Modification

According to RFC 3647, certificate modification is the process of generating new certificates using the same key pair.

This practice is not allowed for Sub-CA and Subscriber certificates. If a new certificate is created, a new key pair is created.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1 Sub-CA

Sub-CA certificate revocation may only be directed by the PMA. In addition to the above, a Sub-CA certificate may be revoked when:

- The RCA or ICA issuing CA in the chain is revoked or ceases activity.
- The subscriber fails to comply with the necessary obligations and security rules in the CP or CPS.
- The subscriber ceases operating, or is otherwise no longer associated with the issuing organization.
- The private key is suspected of compromise or is compromised or is suspected of being compromised.
- Change in policy as directed by the PMA, including requirements for key length, algorithm, validity date, or other certificate attributes.
- Other reasons as directed by the PMA.

4.9.1.2 Subscriber

Not applicable.

4.9.2 Who Can Request Revocation

4.9.2.1 Sub-CA

Only the PMA has the authority to request Sub-CA certificate revocation.

4.9.2.2 Subscriber

Not applicable.

4.9.3 Revocation Request Procedure

4.9.3.1 Sub-CA

The revocation of a Sub-CA certificate shall require the authorization of the PMA. The PMA shall direct the revocation by issuance of a signed document instructing the revocation to the ICA.

The revocation by the ICA shall be performed according to the written procedures of the ICA service provider.

4.9.3.2 Subscriber

Not applicable.

4.9.4 Revocation Request Grace Period

4.9.4.1 Sub-CA

The ICA shall process revocation of Sub-CA certificates upon receipt of direction from the PMA. This revocation shall be processed as quickly as possible not to exceed 10 business days.

4.9.4.2 Subscriber

Not applicable.

4.9.5 Timeframe within which CA Must Process the Revocation Request

4.9.5.1 Sub-CA

The ICA shall process a revocation request as soon as possible after receiving the revocation request, not to exceed 10 business days.

4.9.5.2 Subscriber

Not applicable.

4.9.6 Revocation Checking Requirement for Relying Parties

Use of revoked Certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the Certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a Certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational needs.

4.9.7 CRL Issuance Frequency

CA issues a CRL every 24 hours but CRL.

4.9.8 Maximum Latency for CRLs

CA issues CRL every 24 hours but CRL is valid for 7 days.

4.9.9 On-line Revocation/Status Checking Availability

If CA doesn't include CRL in the signed document, therefore Sub-CAs shall support online status checking (OCSP service) in order to include an OCSP response in the signed document.

4.9.10 On-line Revocation Checking Requirements

The response of the OCSP system for Sub-CA validity status is based on the Sub-CA information.

OCSP shall have the following format:

Field	Requirements
Version	1
Responder ID	OCSP's public key hash
ProducedAT	Date and time of the OCSP response signature
CertID	Subscriber's certificate serialNumber, Sub-CA issuerKeyHash and Sub-CA issuerNameHash
This Update	Date and time of the verification of the Subscriber's certificate status made in the CRL.
Next Update	Date of the next CRL.
CertStatus	"Good", "Revoked" or "unknown"

Field	Requirements
Nonce	Used if and only if the user Application provides a value for this field and reused in full.
Extensions	No extension referenced

4.9.11 Other Forms of Revocation Advertisements Available

Not applicable.

4.9.12 Specific Requirements in the Event of Private Key Compromise

Entities that are authorized to submit alert are required to do so as quickly as possible after being informed of the compromise of the private key.

For Sub-CA Certificates, notification of compromise of private keys shall be performed according to the policies of the ICA service provider.

4.9.13 Suspension of token

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Features

The OCSP service uses the Sub-CA information.

4.10.2 Service Availability

The certificate status service is available according needs of Protect and Sign (Personal signature) service.

4.11 End of Subscription

The contract between Client and OPENTRUST deals with end of relationship.

4.12 Key Escrow and Recovery

4.12.1 Subscriber

4.12.1.1 Which key pair can be escrowed

Not applicable.

4.12.1.2 Who Can Submit a Recovery Application

Not applicable.

4.12.1.3 Recovery Process and Responsibilities

Not applicable.

4.12.1.4 Performing Identification and Authentication

Not applicable.

4.12.1.5 Approval or Rejection of Recovery Applications

Not applicable.

4.12.1.6 KEA and KRA Actions during key pair recovery

Not applicable.

4.12.1.7 KEA and KRA Availability

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

The location and construction of the facility of the OA housing CA, RA and PS equipment shall be consistent with facilities used to house high value and sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards and intrusion sensors, shall provide robust protection against unauthorized access to equipment and records.

5.1.2 Physical Access

CA and RA Equipment shall always be protected from unauthorized access and damage. The physical security mechanisms for equipment at minimum shall be in place to:

- Ensure monitoring, either manually or electronically, of unauthorized intrusion at all times.
- Ensure no unauthorized access to the hardware and activation data is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure location.
- Any non-authorized individual entering secure areas shall always be under oversight by an authorized employee.
- Ensure an access log is maintained and inspected periodically.
- Provide at least three layers of increasing security such as perimeter, building, and operational room.
- Require two person physical access controls for both the cryptographic HSM and activation data for CA.

A security check of the facility housing equipment shall occur if the facility is to be left unattended. At minimum, the check shall verify the following:

- The equipment is in a state appropriate for the current mode of operation.
- For off-line components, all equipment is shut down.
- Any security containers (tamper-proof envelopes, safes ...) are properly secured.
- Physical security systems (e.g., door locks, vent covers, electricity ...) are functioning properly.
- The area is secured against unauthorized access.

Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation data used to access or enable cryptographic modules shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

5.1.3 Power and Air Conditioning

The OA ensures that power and air conditioning facilities are sufficient to support the operation of the PKI system, using primary and back-up installations.

5.1.4 Water Exposures

The OA ensures that systems are protected in a way that minimizes impact from water exposure.

5.1.5 Fire Prevention and Protection

The OA ensures that systems are protected with fire detection and suppression systems.

5.1.6 Media Storage

Media used within the OA are securely handled to protect media from damage, theft and unauthorized access. Media management procedures are implemented to protect against obsolescence and deterioration of media within the period of time that records are required to be retained.

Sensitive data shall be protected against being through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.

CA shall maintain an inventory of all information assets and shall assign a classification for the protection requirements to those assets consistent with the risk analysis.

5.1.7 Waste Disposal

All media used for the storage of sensitive information such as keys, activation data or files shall be destroyed before being released for disposal.

5.1.8 Off-site Backup

Full back-ups of CA systems online, sufficient to enable recovery from system failure, shall be made after PKI deployment according to OPENTRUST policies. Back-up copies of essential business information and software are made regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems shall be regularly tested to ensure that they meet the requirements of the OA business continuity plan (for CA). At least one full back-up copy shall be stored at an offsite location (disaster recovery OA). The back-up copy shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

5.2 Procedural Controls

5.2.1 Trusted Roles

CA shall ensure that roles are defined in order to operate the following set of trusted functions in support of the PKI services (deployed by OpenTrust only) with an appropriate separation of duties:

- Security operation: Owns overall responsibility for managing the implementation of policy practices and CP and defines all the PKI roles and appoints physical person to trusted role.
- PKI system operation: Cleared to install, configure, back-up, recover and maintain PKI systems (off-line and on-line).
- Key management operation: Manages all HSM of the PKI (on-line) and performs key ceremonies (off-line and on-line).
- Audit operation: Authorized to view archives and audit logs produced during the usage and management of the PKI systems (on-line).
- HSM activation: Cleared to hold activation data which are necessary for hardware security module operation (off-line and on-line).
- Key pair protection: Cleared to hold activation data that are necessary for Sub-CA private key management (role different from the HSM activation role).
- On-line PKI Software administration: manage technical roles of the PKI software and configuration of the PKI software.

- On-line PKI software operation: uses the PKI software functionality in order to manage Subscriber's certificate life cycle.

All personnel are formally appointed to trusted roles by the PMA and/or the OA (for CA), as described in the CPS.

Client and DocuSign are responsible to define and documented trusted roles and associated operation. Client shall define trusted role to manage RA and RA personal shall be formally appointed by senior manager.

5.2.2 Number of Persons Required per Task

The number of persons who provide PKI services is detailed in the CPS for CA and Client document for RA. The number of persons is defined to guarantee trust for all services (key generation, certificate generation, revocation, certificate request …), so that no malicious activity may be conducted by a single person acting on behalf of the PKI. All participants shall serve in a trusted role as defined in section 5.2.1 above.

Sub-CA keys are under dual control at minimum.

The following tasks shall be completed by two persons authorized for PKI system operations:

- key generation
- key activation
- key backup
- CA Certificate revocation.

It is forbidden to own privileges (role) for the following operation at the same time:

- An individual owning a role in PKI system operation shall not be involved in any other operation.
- An individual owning a role in security operation shall not be involved in any other operation except Sub-CA HSM activation and Sub-CA Key pair protection.
- An individual owning a role in key management operation shall not be involved in any other operation except Sub-CA HSM activation and Sub-CA Key pair operation.
- An individual owning a role in audit operation shall not be involved in any other operation except security operation.
- An individual owning a role in on-line Sub-CA PKI Software administration shall not be involved in on-line Sub-CA PKI software operation.
- An individual owning a role in Sub-CA HSM activation may be involved in key pair protection if and only if she/he cannot control Sub-CA key pair alone.

Client and DocuSign shall appoint and define role in order to make at least a separation between personal in charge of RA and DocuSign services and personal in charge of RA and DocuSign software to proceed the following operation; configuration, installation, backup, maintain and recovery.

5.2.3 Identification and Authentication for Each Role

All necessary checks must be completed before any individual enters a trusted role within the PKI components.

All persons assigned a role, as described in this CP, are identified and authenticated so as to guarantee that said role enables them to perform their PKI duties. The CPS describes the mechanisms used to identify and authenticate individuals.

5.2.4 Roles Requiring Separation of Duties

Segregation of duties may be enforced using PKI equipment, procedures or both. PKI component employees are individually appointed to trusted roles for operations defined in section 5.2.1 above.

No individual shall be assigned more than one identity unless approved by the PMA.

The part of the CA concerned with certificate generation and revocation management shall be independent of other organizations for its decisions relating to establishing, provisioning and maintaining and suspending of services in conformance with the applicable certificate policies; in particular its senior executive, senior staff and staff in trusted roles, shall be free from any commercial, financial and other pressures which might adversely influence trust in the services it provides.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

PMA and OA components employ a sufficient number of personnel who possess expert knowledge, experience and appropriate qualifications necessary for the job functions and services offered. PKI personnel fulfill the requirements of "expert knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions and clearly identified. PKI personnel sub-contractors have job descriptions defined to ensure separation of duties and least privilege, and position sensitivity is determined based on the duties and access levels, background screening and employee training and awareness. PKI personnel shall be appointed to trusted roles by the PMA.

5.3.2 Background Check Procedures

PMA and OA employees in trusted roles shall be free from conflicting interests that might prejudice the impartiality of the PKI operations. The Client, DocuSign and PMA shall not appoint to trusted roles or management any person who is known to have a conviction for a serious crime or other offence which affects his/her suitability for the position.

5.3.3 Training Requirements

The PMA and OA ensure that all personnel performing duties with respect to operations receive comprehensive training in:

- PKI security principles and mechanisms
- Software versions in use in the PKI system
- PKI business Processes and workflows
- Duties they are expected to perform
- Dispute operations and procedures
- Sufficient IT knowledge.
- Disaster recovery and business continuity procedures

5.3.4 Retraining Frequency and Requirements

Individuals in trusted roles shall be aware of changes in the PKI operations, as applicable. Any significant change to the operations shall be accompanied by a training (awareness) plan, and the execution of said plan shall be documented.

5.3.5 Job Rotation Frequency and Sequence

The PMA and OA Entity ensure that any change in staff will not affect the security of the system.

5.3.6 Sanctions for Unauthorized Actions

Appropriate administrative disciplinary sanctions are applied to any PKI component's personnel violating the OPENTRUST CP.

5.3.7 Independent Contractor Requirements

Contractors employed to perform PKI component functions are subject to the all personnel controls defined in section 5.3. Contractors can perform PKI system operations (refer to section 5.2 above) with approval of the PMA, DocuSign or the Client according the PKI component.

5.3.8 Documentation Supplied to Personnel

PKI components make available to their personnel the present CP and the corresponding CPS, and any relevant statutes and policies. Other technical, operational and administrative documents (e.g., Administrator Manual, User Manual, etc.) are provided to enable the trusted personnel to perform their duties.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Audit log files are generated by OA and PMA for all events related to security and PKI services.

Audit log files are generated for all events related to security and PKI services. Where possible, security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. Each event related to certificate life cycle is logged in such a way that it can be attributed to the person that performed it.

Logging will include the following topics:

- Physical facility access.
- Trusted roles management.
- Logical access.
- Backup management.
- Log management.
- Data from the authentication process for Subscribers and PKI components.
- Date, time, phone number used, persons spoken to, and end results of verification telephone calls.
- Acceptance and rejection of certificate requests.
- Certificate creation.
- Certificate renewal.
- HSM management (for CA and for RA if RA uses HSM).
- Key creation, use and destruction.
- Activation data management.
- Role management.

- IT and network management, as they pertain to the PKI systems.
- PKI documentation management.
- Security management (Successful and unsuccessful PKI system access attempts, PKI and security system actions performed, Security profile changes, System crashes, hardware failures and other anomalies, Firewall and router activities; and entries to and exits from the OA facility).

At minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- Type of event.
- Trusted date and time the event occurred.
- Result of the event: success or failure where appropriate.
- Identity of the entity and/or operator that caused the event.
- Identity for which the event is addressed.
- Cause of the event.

In addition to that, DocuSign as RA portal shall record all the information used:

- To create the certificate request (means all information transmitted to CA and filled by Client for Consent Protocol).
- The result of technical Consent Protocol (Audit file according [SPMP]) as proof of the certificate request enrolled by Client and transmitted to CA.

In addition to that, Client as RA shall record all the information used:

- To verify the subject's identity.
- If applicable, any specific attributes of the subject, including any reference number on the documentation used for verification, and any limitations on its validity (refer to section 3.2 above).
- To create the certificate request (means all information described in section 4.1.2.2 above).
- The list of all RA Operator that are authorized to enroll and manage Subscriber.

5.4.2 Log Processing Frequency

PKI operation audit logs are reviewed on an annual basis by the member of the OA responsible for audits, who conducts a reasonable search for any evidence of malicious activity, and following each important operation.

A statistically significant sample of security audit data generated by their PKI business entity since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity. OA review log on day to day basis for IT and physical security.

The OA shall explain all significant events in log audit report. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews shall be documented.

5.4.3 Retention Period for Audit Logs

Records related to PKI operation are held on the OA site for at least one year before being archived.

5.4.4 Protection of Audit Log

Event logs are protected in such a way that only authorized users can access them.

Events are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to long term media) within the period of time that they are required to be held.

Event logs are protected in such a way so as to remain readable for the duration of their storage period.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed up via enterprise backup mechanisms, under the control of authorized trusted roles, separated from their component source generation. Audit log backups are protected with the same level of trust defined for the original logs.

5.4.6 Audit Collection System (Internal vs. External)

Audit processes shall be invoked at system start up, and end only at system shutdown. The audit collection system has to maintain the integrity and availability of all data collected. If necessary, the audit collection system protects the integrity of the data. If a problem appears during the process of the audit collection system, the PMA determines whether it has to suspend operations until the problem is solved and inform the impacted component.

5.4.7 Event-Causing Subject Notification

Where an event is logged by the audit collection system, it guarantees that the event is linked to a trusted role.

5.4.8 Vulnerability Assessments

The role in charge of conducting audit and roles in charge of realizing PKI system operation explain all significant events in an audit log summary. Such reviews involve verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews are documented.

For vulnerability, the following rules apply:

- Implement detection and prevention controls under the control of the OA to protect PKI systems against viruses and malicious software.
- Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.
- Undergo or perform a vulnerability scan (i) after any system or network changes that the PMA determines are significant for CA and DocuSign, and (ii) at least once per week, on public and private IP addresses identified by the OA as the PKI's systems.
- Undergo a penetration test on the PKI's systems on at least an annual basis and after infrastructure or application upgrades or modifications that the PMA for CA and DocuSign determines are significant.
- Record evidence that each vulnerability scan and penetration test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable vulnerability or penetration test; and
- Track and remediate vulnerabilities according to enterprise cybersecurity policies and risk mitigation methodology.

5.5 Records Archival

5.5.1 Types of Records Archived

PKI component archived records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At minimum, the following data shall be archived for CA:

- PKI events records:
  - Physical facility access log of OA (one year minimum).
  - Video facility access log of OA (one month).
  - Video of key ceremony for CA only (minimum 10 years).
  - Trusted roles management log for OA (minimum 10 years).
  - IT access log for OA (5 years minimum).
  - Subscriber and CA key creation, use and destruction log (minimum 5 years) kept by OpenTrust.
  - Activation data management log for OA (minimum 5 years).
  - IT and network log for OA (minimum 5 years).
  - PKI documentation for OA (minimum 5 years).
  - Security incident and audit report for OA (minimum 10 years).
- PKI audit documentation (minimum 5 years) kept by PMA.
- CP document (minimum 5 years) kept by PMA.
- CPS documents (minimum 5 years) kept by PMA.
- Contract between OPENTRUST and acting RA (minimum 5 years) kept by PMA.
- System equipment, software and configuration (minimum 5 years) for OpenTrust.
- Certificates (or other revocation information) (minimum 5 years) kept by CA.
- Certificate request (minimum of 5 years) records in CA system.
- Other data or applications sufficient to verify archive contents (minimum 5 years).
- All work related to or from the PMA and compliance auditors (minimum 5 years).

RA record for Client, refer to section 5.4.1 above, is archived at minimum 3 years.

DocSign documents its archive duration period.

5.5.2 Archive Retention Period

The minimum retention period for archived data is defined in section 5.5.1 above. The PMA and Client decide, according the archive owner, to delete or keep all or part of the archives at the end of the retention period of each archive.

5.5.3 Archive Protection

The archives are created in such a way that they cannot be easily deleted or destroyed within their defined retention period. Archive protection ensures that only authorized people can access them.

Archives are held in a manner that ensures integrity, authenticity and confidentiality of data.

5.5.4 Archive Backup Procedures

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media will be defined by the archive site.

5.5.5 Requirements for Record Time-Stamping

Time stamping services for PKI are not mandatory.

The records and log data have a trusted time defined by the PKI. Details are given in section 6.8 below.

5.5.6 Archive Collection System (Internal or External)

The archive collection system is compliant with security requirements defined in section 5.4.6.

5.5.7 Procedures to Obtain and Verify Archive Information

Media storing PKI archive information are verified upon creation. Periodically, statistical samples of archived information are tested to check the continued integrity and readability of the information.

Only authorized PMA and OA personnel are allowed to access archives.

5.6 Key Changeover

5.6.1 Sub-CA Certificate

The Sub-CA private key validity period is defined in compliance with cryptographic security recommendations for key size length. The Sub-CA certificate validity period is defined in section 6.3 below.

The Sub-CA cannot generate Subscriber certificates whose validity period would be superior to the Sub-CA certificate validity period. A new key pair for the Sub-CA requires a new Sub-CA certificate be generated.

The Subscriber certificate has a fixed validity period which cannot be changed due to end of life of Sub-CA.

As soon as a new key pair is generated for the Sub-CA, only the new private key is used to sign Subscriber certificates.

Previous Sub-CA certificates shall be used for the validation process of the certification path for all Subscriber certificates signed by the previous Subscriber.

The PMA reserves the right to change the key at any time.

5.6.2 Subscriber Certificate

The Subscriber private key validity period is defined in compliance with cryptographic security recommendations for key size length. The Subscriber certificate validity period is defined in the CA CP.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

This system shall be supported by the OPENTRUST enterprise computing infrastructure and its incident, compromise and business continuity plans. These plans shall be periodically tested, reviewed and updated, as directed by the OPENTRUST.

If a PKI component (for OpenTrust) detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. The scope of potential damage is assessed by the PMA in order to determine if the PKI needs to be rebuilt, if only some certificates need to be revoked, and/or if the PKI has been compromised. In addition, the PMA determines which services are to be maintained (revocation and certificate status information) and how, in accordance with the PMA business continuity plan.

Incident, Compromise and Business continuity are covered in the CPS, which may also rely upon other enterprise resources and plans for implementation.

If a RA component (for Client and DocuSign) detects a potential hacking attempt or other form of compromise, it performs an investigation in order to determine the nature and the degree of damage. The scope of potential damage is assessed by the Client and/or DocuSign in order to determine if the RA needs to be rebuilt, if only some certificates need to be revoked, and/or if the RA has been compromised. In addition, the Client and/or DocuSign determines which services are to be maintained and how, in accordance with the Client business continuity plan. Client and/or DocuSign shall alert PMA in case of RA compromission.

Incident, Compromise and Business continuity are covered in the Client and DocuSign documentation, which may also rely upon other enterprise resources and plans for implementation.

5.7.2 Corruption of Computing Resources, Software, and/or Data

If PKI equipment is damaged or rendered inoperative, but signature keys are not destroyed, the operation is re-established as quickly as possible, with priority given to the ability to generate certificate status information.

5.7.3 Entity Private Key Compromise Procedures

If a CA key is compromised, lost, destroyed or suspected of being compromised:

- The PMA investigates on the “key-issue” and revokes the associated certificate.
- A new key pair is generated and a new certificate is created.
- Alert the Client.

If system used by Protect and Sign (Personal signature) service to generate Subscriber key pair is compromised, then PMA alert the Client and gives a list of detailed risk and consequence for Client and Subscriber due to the compromising.

When any of the algorithms, or associated parameters, used by the CA or its Subscriber becomes insufficient for its remaining intended usage then the CA shall inform the Client and change the used algorithms.

5.7.4 Business Continuity Capabilities after Disaster

The business continuity plan addresses all necessary operations as described in section 5.7.1 above.

5.8 Termination

5.8.1 Sub-CA

In the event of the termination of the PKI service, the PMA provides notice prior to the termination, and:

- Inform Client according Client contract terms.
- Destroys the Sub-CA private key.
- Publishes the most recent revocation status information (CRL signed by CA) to all Relying parties (if any).
- The Sub-CA signed by the ICA stops delivering certificates in accordance with and referring to this CP and in accordance with its CP.
- In the case of a compromised Sub-CA, the PMA and OA both use secure means to notify Subscribers and relying parties that they must delete all trust certificates representing the Sub-CA with the compromised(s) key pair(s).
- Archives all audit logs and other records prior to terminating the PKI.
- Archived records are transferred to the PMA.

In the event of the termination of the OA services, the OA is responsible for keeping all relevant records regarding the needs of Subscriber and PKI components. The OA then transmits its records to the PMA.

5.8.2 RA

In the event of the termination of the RA service on Client request, the Client provides notice prior to the termination, and:

- Inform PMA and DocuSign by register letter.
- The RA stops delivering certificates request to the CA for the Client.
- In the case of a compromised RA, the Client and DocuSign use secure means to notify Subscribers and relying parties that they must not trust Subscriber certificate identified in the list provided by Client.

- Archives all audit logs and other records prior to terminating the PKI.
- Archived records are transferred to an entity designated by Client.

In the event of the termination of the OA services, the OA is responsible for keeping all relevant records regarding the needs of Subscriber and PKI components. The OA then transmits its records to the Client. Client contract defines the rules in case of DocuSign termination and/or Client termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 Sub-CA

After the PMA agrees to the generation of the Sub-CA, a key pair and CSR are generated for the Sub-CA.

The operation of the Sub-CA key pair and CSR generation is video-recorded and performed according to a key ceremony script. The HSM used for the key ceremony is compliant with requirements defined in section 6.2.1 below.

Sub-CA key pair generation is undertaken and witnessed in a physically secure environment (refer to section 5.1 above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision. Private Key activation data are distributed to activation data holders that are trusted employees. Sub-CA key generation is carried out within a hardware security module (refer to section 6.2 below). Witnesses are persons other than the operational personnel. Sub-CA HSM activation and initialization is under the control of Sub-CA activation data holders. During the key ceremony, the Sub-CA key pair is backed up (refer to section 6.2. below).

6.1.1.2 Subscriber

Protect and Sign (Personal Signature), refer to [PSPM], generates the Subscriber key pair. The generation is performed using a HSM (refer to section 6.2 below). The generation shall be performed in such a way as to avoid compromising the private key and associated activation data and avoid non required signature operation. The private key shall be protected with the associated activation data.

6.1.2 Private Key Delivery

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

6.1.3.1 Sub-CA

Sub-CA public keys are securely delivered to the relevant ICA for certificate issuance during key ceremonies (for PKI set-up) or during the registration process (refer to section 4.1 and 4.2 above). The delivery mechanism binds Sub-CA checked identities to the public keys to be certified using the Pkcs#10 format.

6.1.3.2 Subscriber

A Subscriber's public key is securely delivered by Protect and Sign (Personal Signature) platform (refer to [SPMP]) software to the Sub-CA for certificate issuance. The delivery mechanism binds the transmitted identities to the public keys to be certified using the Pkcs#10 format.

6.1.4 CA Public Key Delivery to Relying Parties

Refer to section 2 above.

6.1.5 Key Sizes

6.1.5.1 Sub-CA

The key pair is 2048 bits long for the RSA algorithm.

RSA algorithm is used with SHA-2 as hash function.

6.1.5.2 Subscriber

The key pair is 2048 bits long for the RSA algorithm.

RSA algorithm is used with SHA-2 as hash function.

6.1.6 Public Key Parameters Generation and Quality Checking

6.1.6.1 Sub-CA

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto-algorithm for the parameters that are to be used.

Sub-CA keys are generated in accordance with the cryptography tools of the hardware security modules (refer to section 6.2 below).

6.1.6.2 Subscriber

Public key parameters shall always be generated and checked in accordance with the standard that defines the crypto-algorithm in which the parameters are to be used.

Subscriber keys are generated in accordance with the cryptography tools of the hardware security modules or tokens used to protect the keys (refer to section 6.2 below).

6.1.7 Key Usage Purpose (as per X.509 v3 key usage field)

The use of a specific key is determined by the keyUsage extension in the X.509 Certificate. The Certificate Profiles in section 10 below specify the allowable values for this extension for different types of Certificates defined under this CP, and all Sub-CAs issuing Certificates in accordance with this CP must adhere to those values.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

6.2.1.1 Sub-CA

The Sub-CA generates its key pairs and stores their private keys within an HSM that is certified according to the rating specified in section 6.2 below.

6.2.1.2 Subscriber

Key pairs are generated and stored within an HSM or a token that is certified according to the rating specified in section 6.2 below.

6.2.2 Private Key (N out of M) Multi-Person Control

6.2.2.1 Sub-CA

The Sub-CA implements technical and procedural mechanisms that require the participation of multiple trusted individual authorizations to perform sensitive Sub-CA cryptographic operations.

6.2.2.2 Subscriber

Subscriber's key pair is activated on RA request after successful authentication of the Subscriber using its activation data according Consent Protocol chosen by Client and performed by RA.

6.2.3 Private Key Escrow

6.2.3.1 Sub-CA

Under no circumstances shall a Sub-CA private key be escrowed by any PKI component or third party.

6.2.3.2 Subscriber

Under no circumstances shall the private key be escrowed by a third party or by PKI components.

6.2.4 Private Key Backup

6.2.4.1 Sub-CA

Sub-CA private signature keys shall be backed up under the same multi-person control as the operational ones. A single back-up copy of the signature key shall be stored in the Sub-CA systems location. A second back-up copy shall be kept at the Sub-CA off-site backup location. All locations must be accepted by the PMA.

6.2.4.2 Subscriber

Not applicable.

6.2.5 Private Key Archival

6.2.5.1 Sub-CA

Sub-CA private keys shall never be archived.

6.2.5.2 Subscriber

Not applicable.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

6.2.6.1 CA Private Key

In the case of private key transfer, the Sub-CA key pair is transferred to another Hardware Security Module (HSM) of the same specification as described in section 6.2, by direct token-to-token copy, via a trusted path under N out of M multi-person control (refer to section 6.2).

Sub-CA keys are generated, activated and stored in HSMs or in an encrypted format. When they are not stored onto HSMs, Sub-CA private keys are encrypted. An encrypted Sub-CA private key cannot be decrypted without using an HSM with the required trusted role (activation data holder), and must be performed in the presence of multiple persons in trusted roles.

6.2.6.2 Subscriber

Not applicable.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 Sub-CA

The HSM may store Private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with those mentioned in the security policy attached to the approved HSM.

6.2.7.2 Subscriber

Dedicated HSM in OpenTrust's data center for Protect and Sign (Personal signature) service stores Subscriber's private Keys in any form as long as the keys are not accessible without authentication mechanisms that are compliant with those mentioned in the security policy attached to the approved HSM.

6.2.8 Method of Activating Private Key

6.2.8.1 Sub-CA

Several trusted roles with activation data are required to perform the initial activation of the HSM that contains the Sub-CA key pair corresponding to a Sub-CA Certificate. Once the HSM containing the Sub-CA key and the Sub-CA key are operational, only the authorized services of the PKI system can use the Sub-CA key pair within the HSM, by using the mutual authenticated interface of the PKI systems.

6.2.8.2 Subscriber

After successful authentication of Subscriber by RA during Consent Protocol, RA transmits technical certificate and signature request to Protect and Sign (Personal Signature) platform as defined in [SPMP].

Protect and Sign (Personal Signature) platform authenticates RA, generates (refer to section 6.1.1.2 above), transmits CSR to CA (refer to section 6.1.3 above) and then activates Subscriber private key in order to use to sign document as defined in [SPMP].

6.2.9 Method of Deactivating Private Key

6.2.9.1 Sub-CA

A Sub-CA HSM that has been activated is never left available to unauthorized access.

After being used, HSMs are deactivated. After deactivation, the use of the HSM-based Sub-CA key pair shall require the presence of the trusted roles with the activation data in order to reactivate said Sub-CA key pair (refer to section 6.2).

The HSM automatically deactivate the HSM if there is an incident.

6.2.9.2 Subscriber

Subscriber's key pair is used to sign fingerprint of document on request of RA, according [PSPM] and Client Consent Protocol and Client Signature Policy, and destroyed immediately after usage.

6.2.10 Method of Destroying Private Key

6.2.10.1 Sub-CA

Destroying a Sub-CA private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization function of hardware in such a way that no information can be used to recover any part of the private key. All the Sub-CA private key back-ups must be destroyed using the same level of security. If the HSM functions are not accessible in order to destroy the key contained inside, then the HSM has to be physically destroyed.

The destruction operation is realized in a physically secure environment (refer to section 5.1above) by personnel in trusted roles (refer to section 5.2 above) under at least dual supervision.

6.2.10.2 Subscriber

Destroying a Subscriber's private key inside an HSM requires destroying the key(s) inside the HSM using the zeroization function of hardware in such a way that no information can be used to recover any part of the private key. If the HSM functions are not accessible in order to destroy the key contained inside, then the HSM has to be physically destroyed.

6.2.11 Cryptographic Module Rating

6.2.11.1 Sub-CA

The Hardware Security Module used to generate RCA key pairs is at least approved in accordance with FIPS 140 - 2 Level 3 standard or EAL4+ Common Criteria equivalent.

6.2.11.2 Subscriber

The Hardware Security Module used to generate OCSP key pairs is at least approved in accordance with FIPS 140 - 2 Level 2 standard or EAL4+ Common Criteria equivalent.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Public keys are archived as part of certificate archival as described in section 5.5 above.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

6.3.2.1 Sub-CA

The maximum operational period for a Sub-CA private key is five (5) years.

The maximum operational period for a Sub-CA certificate is 5 (5) years.

6.3.2.2 Subscriber

A Subscriber private key can be used as long as the associated certificate is valid, and can be used for decrypting encrypted data as long as is necessary.

The Subscriber certificate validity period is given in section 10.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

6.4.1.1 Sub-CA

Sub-CA activation data used to protect HSM containing Sub-CA private keys are generated during the initial PKI key ceremony. The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys. Some of the most critical activation data are backup (CPS gives exact details).

The PMA-appointed individuals shall receive their activation data during the key ceremony through a face-to-face meeting. Creation and distribution of activation data are logged. The activation data are never transmitted by any other means.

6.4.1.2 Subscriber

The Consent Protocol (refer to section 4.3 above) may require a technical activation data (for example: OTP code…).

When activation data is requested, this activation data is generated either by RA platform or by Client (for example, Client can create a code and give it to Subscriber). When an activation data is generated by Client, then this activation data shall be securely transmit to the RA and Subscriber in order to be used by RA to authenticate Subscriber. When DocuSign creates activation data, it is done according DocuSign policy.

6.4.2 Activation Data Protection

6.4.2.1 Sub-CA

Activation data is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

The PMA requires that activation data holders store their activation data in a safe for which access is controlled by both the holder and other employees in trusted roles.

If activation data is written on paper, then the paper has to be stored securely in a safe.

6.4.2.2 Subscriber

A Subscriber is responsible for ensuring the protection of his/her activation data.

When activation data are managed by Client and/or RA then these entities are also responsible of the protection of the protection of the activation data in a way to avoid use of activation data by other entity than the Subscriber.

6.4.3 Other Aspects of Activation Data

6.4.3.1 CA

Activation data are changed if hardware security modules are re-keyed or returned to the manufacturer for maintenance. Other aspects of activation data management are given in the CPS.

6.4.3.2 Subscriber (physical person)

Not applicable.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards. PKI components implement the following functionalities (CA and RA IT system when applicable):

- Require authenticated logins for trusted roles.
- Provide discretionary access control.
- Require use of authentication for session communication.
- Require user identification.
- Provide domain isolation for processes involving roles using PKI services.
- Remove unwanted services and ports from the PKI components.

When the PKI equipment is hosted on platforms certified for computer security assurance requirements, the system (hardware, software and operating system), when possible, operates in said certified configuration. At minimum, such platforms use the same version of the computer operating system as the one which received the evaluation rating. OA computer systems are configured with minimum required accounts, network services, and no remote login.

Sub-CA key pair generation is performed on the online HSMs, except during PKI system set-up where the HSM used online will be set up in an offline environment.

Key ceremony workstations are dedicated to key ceremony operations and not connected to any public network. Computers used in the administration of the PKI systems are dedicated to this task only.

The following rules apply for CA and RA:

- Follow a documented procedure for appointing individuals to trusted roles and assigning responsibilities to them on each PKI component.

- Document the responsibilities and tasks assigned to trusted roles and implement “separation of duties” for said trusted roles based on the security-related concerns of the functions to be performed on each PKI component.

- Ensure that only personnel assigned to trusted roles have access to PKI components.

- Ensure that an individual in a trusted role acts only within the scope of said role when performing administrative tasks assigned to that role on the PKI component.

- Require employees and contractors to observe the principle of “least privilege” when accessing, or when configuring access privileges on PKI system (refer to section 5.2 above).

- Require that each individual in a trusted role use a unique credential (strong password, certificate…) created by or assigned to that person in order to authenticate to PKI component.

- If an authentication control used by a trusted role is a username and password, then the handling of those authentications shall be performed in accordance with corporate enterprise security policy.

- Require trusted roles to log out from the PKI service of the PKI component and lock workstations when no longer in use.

- Configure workstations with inactivity time-outs that log the user off and lock the workstation after a set time of inactivity without input from the user (PKI components allow a workstation to remain active and

unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock).

- Review all system accounts and deactivate any accounts that are no longer necessary for operations.
- If applicable for a PKI component (means only for a PKI component that uses a different access control system than a certificate for a trusted role) lockout account access to the PKI component after no more than a defined maximum value of failed access attempts, provided that this security measure is supported by the PKI component and does not weaken the security of this authentication control.
- Implement a process that disables all privileged access of an individual to the PKI component within 24 hours upon termination of the individual's (with trusted role) employment or contracting relationship with the PKI component.

6.5.2 Computer Security Rating

No stipulations.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the PKI are as follows:

- Use software that has been designed and developed under a formal, documented development methodology according to Common Criteria evaluation (for CA).
- Hardware and software procured shall be purchased in such a way so as to reduce the likelihood that any particular component was tampered with.
- Hardware and software shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.
- All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location.
- The hardware and software shall be dedicated to performing the PKI activities. There shall be no other applications; hardware devices, network connections, or component software installed which are not part of the PKI operation.
- Proper care shall be taken to prevent malicious software from being loaded onto the equipment.

Only applications required to perform the PKI operations shall be obtained from sources authorized by local policy. PKI hardware and software shall be scanned for malicious code on first use and periodically thereafter.

Hardware and software updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the PKI system as well as any modifications and upgrades shall be documented and controlled. A procedure shall be used for installation and ongoing maintenance of the PKI system. The PKI software shall be verified as being that supplied from the vendor, with no modifications, and be the version

intended for use. There shall be a mechanism for detecting unauthorized modification to software or configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance for the system.

The following rules apply:

- Implement an IT administration system under the control of the OA that monitors, detects, and reports any security-related configuration change to PKI systems.
- Require trusted role personnel to follow up on alerts of possible critical security events.
- Conduct a human review of application and system logs and ensure that monitoring, logging, alerting, and log-integrity-verification functions are operating properly (refer to section 5.4.8 above).

6.6.3 Life Cycle Security Controls

For the software and hardware that are evaluated, the PMA monitors the maintenance scheme requirements to ensure the same level of trust.

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

6.7 Network Security Controls

The PKI system shall implement appropriate security measures to ensure they are guarded against denial of service and intrusion attacks. Such measures shall include the use of guards, firewalls and filtering routers. Unused network ports and services shall be turned off. Any network software present shall be necessary to the functioning of the PKI system.

The following rules apply:

- Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.
- Segment PKI equipment into networks or zones based on their functional, logical, and physical (including location) relationship. Only authorized flow, used for administration and PKI services, between PKI equipment shall be authorized.
- Maintain and protect PKI components in at dedicated zone (RA is separated from CA) and make a separation between interfaces accessible from Internet to interfaces accessible by internal needs.
- Implement and configure an administration network (a system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, anti-virus when it is applicable and IT administration) that protects systems and communications between PKI systems and communications with non-PKI systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks.
- Configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the PKI component has identified as necessary to its operations.

- Configure PKI components by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the PKI component's operations and allowing only those that are approved by the PKI component.

- Grant administration access to PKI components only to persons acting in trusted roles and require their accountability for the PKI component's security.

- Implement authentication mechanism for each trusted role of each component of the PKI.

- Change authentication keys and passwords for any privileged account or service account on a PKI System whenever a person's authorization to administratively access that account on the PKI System is changed or revoked.

- Apply recommended security patches, viewed by the software editor and entity like CERT as mandatory to avoid a concrete and high risk attack on the PKI system, with to PKI systems within six months of the security patch's availability, unless the PKI establishes that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

6.8 Time-Stamping

Electronic or manual procedures shall be used to maintain system time. Clock adjustments are auditable events as listed in section 5.4 above. Key ceremony uses a manual procedure.

For secured time on audit records, all Sub-CA system components shall regularly synchronize with a time service such as Network Time Protocol (NTP) Service. Time derived from the time service shall be used for establishing the time of:

- Initial validity time of a Subscriber Certificate.

- Initial validity time of CRL and OCSP response.

Additional information is given in the applicable CPS. Client and RA shall take care about the RA system to control system time.

7 CERTIFICATE, CRL AND OCSP PROFILES

7.1 Certificate Profile

7.1.1 Version Numbers

Issued certificates are X.509 v3 Certificates (populate version field with integer "2").

7.1.2 Certificate Extensions

Any Sub-CA asserting critical private extensions shall be interoperable in their intended community of use.

Issuer Sub-CA and Subscriber Certificates may include any extensions as specified by RFC 5280 in a Certificate, but must include those extensions required by this CP. Any optional or additional extensions shall be non-critical and shall not conflict with the Certificate and CRL profiles defined in this CP. Section 10 contains these Certificate profiles.

7.1.3 Algorithm Object Identifiers

Certificates issued under this CP shall use the following OIDs for signatures:

sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(11)}

Certificates issued under this CP shall use the following OIDs for signatures:

Sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha256WithRSAEncryption(5)}

Certificates under this CP shall use the following OID for identifying the subject public key information:

rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.4 Name Forms

The Subject and Issuer fields of the Certificate shall be populated with a unique Distinguished Name in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by [RFC5280] and section 3.1.

7.1.5 Name Constraints

The Sub-CA asserts critical or non-critical name constraints beyond those specified in the Certificate profiles in section 10 below for the Sub-CA certificate and Subscriber Certificate.

7.1.6 Certificate Policy Object Identifier

Refer to section 10 below.

7.1.7 Usage of Policy Constraints Extension

Not applicable.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this CP may contain policy qualifiers such as user notice, policy name, and CP and CPS pointers as described in section 10 below.

7.1.9 Processing Semantics for the Critical Certificate Policy Extension

Processing semantics for the critical Certificate policy extension shall conform to X.509 certification path processing rules as described in section 10 below.

7.2 CRL Profile

Refer to section 10 below.

7.3 OCSP Profile

Refer to section 10 below.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

The PKI components are subject to periodic compliance audits, to allow the PMA to authorize or not (based on the audit result) PKI components hosted by the OA to operate under this CP according to the "PKI audit guide" provided by the PMA.

The PMA has the right to require non periodic compliance audit of PKI components (especially RA) that operate under this CP. The PMA states the reason for any non-periodic compliance audit.

8.2 Identity/Qualifications of Assessor

Compliance auditors shall demonstrate competence in the field of compliance audits and shall be thoroughly familiar with requirements of these CP. Compliance auditors must perform such compliance audits as a primary responsibility. The PMA should carefully review the methods employed to audit PKI components for its own audit requirements base. The PMA is responsible for selecting the auditor for its own PKI components. In addition, the PMA must approve selected auditors.

The compliance auditor is either a private firm, which is independent from the entity being audited, or sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation.

The PMA determines whether a compliance auditor meets these requirements in order to audit CA and RA.

8.3 Topics Covered by Assessment

The purpose of a compliance audit shall be to verify that a component operates in accordance with this CP and the corresponding CPS.

For CA, the perimeter of audit is OA, CA, Client contractual relationship and RA control by PMA.

For RA, the perimeter of audit is:

- DocuSign:
  - DocuSign perimeter for audit is defined in the contract between DocuSign and OpenTrust.
- Client:
  - If applicable, the connection between the RA's and the DRAs'.
  - IT and physical protection of the environment hosting the RA's platform (and, if applicable, the DRAs' platform) used to manage Subscriber's information transmitted to DocuSign platform and prepare electronic document to be signed.
  - Registration Policy content and rules defined to authenticate, identified and stored all elements used to verify Subscriber identity.
  - Protection of means and data used to have access to Client's dedicated account in DocuSign service.
  - Management of electronic documents and signed document.
  - RA monitoring of DRAs (if the RA has designated DRAs) in accordance with the Registration Policy and the contract between the RA and each DRA.
  - Requirements to be met by DRAs regarding User authentication and identification and the secure transmission of User identification data to the RA by DRAs.

8.4 Actions Taken as a Result of Deficiency

The PMA may determine that PKI components do not comply with obligations set forth in this CP. In the case of non-compliance, the PMA may suspend operation of the non-compliant PKI component, or may decide to discontinue relations with the affected PKI component, or decide that other corrective actions have to be taken.

When the compliance auditor finds a discrepancy with the requirements of this CP, the following actions shall be performed:

- The compliance auditor notes the discrepancy.
- The compliance auditor notifies the Entity of the discrepancy. The auditor and the Entity shall notify the PMA promptly.
- The party responsible for correcting the discrepancy determines what further notifications or actions are necessary pursuant to the requirements of this CP, and then proceeds to make such notifications and take such actions without delay in relation with the approval of PMA.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the PMA may decide to temporarily halt operation of a PKI component (typically end relationship with a Client temporally or definitively), to revoke a certificate issued by the PKI component, or take other actions it deems appropriate. Based on the audit result the PMA can decide to revoke CA.

8.5 Communication of Results

An Audit Compliance Report, including identification of corrective measures taken or being taken by the component, is provided to the PMA as well as the dedicated persons in the entity. The report identifies the versions of the CP and CPS and any other auditing criteria used as the basis for assessment.

The Audit Compliance Report is not available on the Internet for relying parties. However, it may be provided to law of court or any official body based on legal request. In addition, it should be available, in part or in whole, to the Audited entity according to the PMA decision.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

These services are defined in the Client Contract.

9.1.2 Certificate Access Fees

No fees.

9.1.3 Revocation or Status Information Access Fees

Not applicable.

9.1.4 Fees for Other Services

These services are defined in the Client Contract.

9.1.5 Refund Policy

These services are defined in the Client Contract.

9.1.6 Fines List

These services are defined in the Client Contract.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

OPENTRUST maintains reasonable levels of insurance coverage.

9.2.2 Other Assets

OPENTRUST maintains sufficient financial resources to maintain operations and fulfill PKI services.

9.2.3 Insurance or Warranty Coverage for Subscribers

If there is damage for a Client due to OPENTRUST fault, OPENTRUST will activate its insurance to cover part of the Client damage in the limits stated in Client Contract.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

PMA guarantees a special treatment for the following confidential information:

- Records and archive of OA.
- Personal identity data.
- Sub-CA private keys.
- Subscriber private key.
- Subscriber certificate request.
- Sub-CA activation data.
- Audit result and reports.

- Business continuity plan.
- Contractual and agreement with Client.
- Internal facility security policy.
- CPS.

The treatment of confidential business information provided by RA and Client in the context of submitting a certificate request for Subscriber will be in accordance with the terms of the Client Contract.

Each RA and Client shall maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential or by its nature should reasonably be understood to be confidential, and shall treat such information with the same degree of care and security as the CA treats its own most confidential information.

9.3.2 Information Not Within the Scope of Confidential Information

All information that is published by the PS (CP and CA certificates) is considered to be not confidential.

9.3.3 Responsibility to Protect Confidential Information

PKI components shall be responsible for protecting the confidential information they possess in accordance with the applicable laws and contracts. PKI components must not disclose certificate or certificate-related information to any third party unless authorized by this policy, required by law, government rule or regulation, or order of a court of competent jurisdiction.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

For the purposes of the PKI related services, PKI components may collect, store, or process personally identifiable information. Any such use or disclosure shall be in accordance with applicable laws and regulations, specifically the European Data Protection Act and the present Certification Policy.

OpenTrust manage Subscriber personal data according applicable laws and regulations, specifically the European Data Protection Act and the present Certification Policy.

Entity RAs shall develop a privacy policy, according to European Law, and stipulate in the contract between Client and OPENTRUST how they protect any personally identifiable information they collect.

Subscribers must be given access and the ability to correct or modify their personal or organization information upon appropriate request to the Client according DocuSign policy and Client rules. Such information must be provided only after taking proper steps to authenticate the identity of the requesting party.

When personal or organization information for Subscriber's has to be modified, then it shall be done before certificate generation. Once the Subscriber certificate is generated, it is not possible for Subscriber to request modification and deletion of RA and CA record that concerned its private personal data. Client is the sole point of contact for the Subscriber to have access to its personal data according Client terms and condition.

9.4.2 Information Treated as Private

The Subscriber information must be treated as private as well as any information protected under national law of the Sub-CA and RA.

9.4.3 Information Not Deemed Private

Any and all information within a certificate is inherently public information and shall not be considered confidential information.

9.4.4 Responsibility to Protect Private Information

PMA, OA and PKI component shall have the responsibility to protect private information and shall refrain from disclosing it unless by order of the Sub-CA and RA pursuant to law enforcement.

9.4.5 Notice and Consent to use Private Information

All private information coming from a PKI component cannot be used without any explicit consent from the Subscriber (refer to section 4.1) and PMC for dedicated treatment.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Sub-CA is compliant with its national law and has secure procedures to clear access to private data.

RA is compliant with its national law and has secure procedures to clear access to private data.

9.4.7 Other Information Disclosure Circumstances

The PMA obtains consent from PKI Components to transfer its private data in case of a transfer of activity as described in section 5.8.

9.5 Intellectual Property Rights

The PMA shall maintain intellectual ownership of CA certificates that it publishes. This CP shall be the property of the PMA. Any service mark, trademark, or trade name contained within a certificate or certificate application shall remain the property of its owner. The Sub-CA key-pairs and corresponding certificate shall be the property of the PMA.

9.6 Representations and Warranties

9.6.1 PMA Representations and Warranties

The PMA defines the present CP and the corresponding CPS. The PMA establishes that PKI components are compliant with the present CP. The processes, procedures and audit framework used to determine compliance are documented within the CPS.

The PMA ensures that all requirements on a PKI component, as detailed in the present CP and in the corresponding CPS, are implemented as applicable to deliver and manage certification services.

The PMA has the responsibility for compliance with the procedures prescribed in this CP, even when PKI component functionality is undertaken by sub-contractors. PKI components provide all their certification services consistent with their CPS.

The PMA has the responsibility to audit the RA and approve RA's procedures to control that Client (RA) acting well according the present CP.

9.6.2 Sub-CA Representations and Warranties

The Sub-CA has the responsibility to:

- Protect and guarantee integrity and confidentiality of their activation data and/or private key.
- Only use their private key and certificate, with associated tools specified in CPS, for what purpose they have been generated.
- Respect and operate the section(s) of the CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).
- Allow the auditor team to control and check the compliance with the present CP and with the components CP/CPS and communicate the requested information to them, in accordance with the intentions of the PMA.

- Document their internal procedures to complete the global CPS.
- Use every means (technical and human) necessary to achieve the realization of the CP/CPS it has to implement and for which they are responsible.
- If the Subscriber's private key has been lost, stolen potentially compromised due to compromise of activation data or other reason notify Client.
- Shall carry out a risk assessment to evaluate business risks and determine the necessary security requirements and operational procedures. The risk analysis shall be regularly reviewed and revised if necessary.
- Shall implement and define CP and CPS according principals set in OPENTRUST security policy.

9.6.3 RA Representations and Warranties

The RA has the responsibility to:

- Ensure that evidence of Subscriber's and subject's identification and accuracy of their names and associated data are either properly examined as part of the defined service or, where applicable, concluded through examination of attestation from appropriate and authorized sources, and that certificate requests are accurate, authorized and complete according to the collected evidence or attestation.
- Before entering into a contractual relationship with a subscriber, the RA shall inform the subscriber of the terms and condition regarding use of the certificate. The RA shall communicate this information though a durable (i.e. with integrity over time) means of communication, which may be transmitted electronically, and in readily understandable language.
- Submit accurate and complete information to the CA in the certificate request according PSMP document.
- Make Subscriber be able to view information that will be set in Subscriber certificate to create its identity (refer to section 4.3 above) during Consent Protocol.
- Make CA's terms and conditions shown to the Subscriber during the Consent Protocol and accepted by Subscriber during the Consent Protocol.
- Let auditor team audit and communicate the requested information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS and the RA procedure.
- Alert PMA when there is a security incident about the RA services that the OA performed.
- Respect the CP and corresponding CPS.
- Protect its information system and guaranty the security of the data transmitted to the PKI.
- Collect and verify Subscriber information in order to create the Subscriber certificate.
- Implement and perform the Consent Protocol and create associated Audit file.
- Records and archive.
- Authenticates and identify the Subscriber.
- Submit accurate and complete information about the Subscriber to the Sub-CA.
- Protect information of the Subscriber.
- Exercise reasonable care to avoid unauthorized use of the subject's private key.
- Designate and maintain a list of all RA Operator.
- Alert Client in case of incident related to CP and RA procedure.
- Respect Client Contract.

9.6.4 Client Representations and Warranties

Make available the signed document to the Subscriber.

- Exercise reasonable care to avoid unauthorized use of the private key of Subscriber.
- Notify Subscriber in case of Client private key has been potentially compromised due to compromise of activation data or other reason.
- Notify Subscriber in case of Subscriber private key has been potentially compromised due to compromise of activation data or other reason.

- In case of being informed that the CA which issued the Subscriber's certificate has been compromised, ensure that the certificate is not used by the Subscriber or a Relying Party.
- Establishes contract with RA and OA entity when they are different legal entity from it with clear identification of PKI services run by the entity and all RA's and OA's obligations and warranties according PKI services managed.
- Defines RA procedure and RA management procedure.
- Alert PMA in case of incident due to RA.
- Select and defines Consent Protocol.
- Respect the CP and corresponding CPS.
- Protect its information system and guaranty the security of the data transmitted to the PKI.
- Let auditor team audit and communicate the requested information to them, according to the PMA intention, control and check the compliance with the present CP and with the components CPS, the Client Contract, the RA procedure and [SPMP].

9.6.5 OA Representations and Warranties

The OA has the responsibility to:

- Respect its security policy.
- Protect and guarantee integrity and confidentiality of their secret data and/or private key.
- Allow the auditor team to control and check the compliance with the present CP/ auditing criteria and components of the CPS as well as the OA's security policy and communicate every useful piece of information to them, in accordance with the intentions of the PMA.
- Alert PMA when there is a security incident with the PKI services that the OA performed.
- Respect and operate the section(s) of the CPS that deals with their duties (this part of CPS has to be transmitted to the corresponding component).
- Protect identity token and associated activation data.
- Protect and guarantee integrity and confidentiality of their secret data and/or private key.
- Document their internal procedures to complete the global CPS and its security policy.
- Respect the total or parts of the agreement(s) that binds it to the PMA and to the Client.

9.6.6 Subscriber

The physical person has the responsibility to:

- Accurately represent themselves in all communications with the RA.
- Only use activation data through the RA application according the Consent Protocol.
- When they are used, protect their activation data at all times and prevent them from unauthorized access in accordance with this policy, as stipulated in the CA's GTU and DocuSign's GTU.

- Abide by all the terms, conditions, and restrictions levied on the use of their Certificates, as set forth in this CP and the Subscriber agreement.

- Use Certificates provided by the Sub-CA only for authorized and legal purposes in accordance with the Entity CP.

- Cease to use such issued Certificates if they become invalid and remove them from any applications they have been installed on.

9.6.7 Representations and Warranties of Other Participants

9.6.7.1 Relying Party Representations and Warranties

Any relying party has the responsibility to validate a digital certificate using:

- Only accept the use of the Certificate for the purposes indicated in the Certificate keyUsage extensions.
- Verify the validity of the Certificate, using the procedures described in [RFC5280], prior to any reliance on said Certificate.
- Check the OID contained in each certificate of the trusted certification path in order to be sure to accept the right kind of certificate.
- Establish trust in the Sub-CA who issued the Certificate by the methods outlined elsewhere in this CP, and using the path validation algorithm outlined in [RFC5280].
- Preserve the original signed data, the applications necessary to read and process that data and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify said signature.
- Cease to use such issued Certificates (Subscriber, Sub-CA ...) if they become invalid and remove them from any applications they have been installed on.

9.7 Disclaimers of Warranties

The PMA guarantees through the PKI services:

- Identification and authentication of Sub-CA, with the Sub-CA Certificate generated by the ICA.
- Management of corresponding certificates and certificate status information regarding the present CP.
- Subscriber certificate content according RA transmitted information about Subscriber.
- Subscriber key pair generation and usage.

The RA guarantees trough the PKI services:

- Identification and authentication of Subscriber, with Subscriber certificate generated by the applicable Sub-CA.
- When it is applicable, transmission of activation data to the right Subscriber.
- Consent protocol operation for Subscriber and certificate transmission to CA.

PMA provides no warranty, express, or implied, statutory or otherwise and disclaims any and all liability for the success or failure of the deployment of the PKI or for the legal validity, acceptance or any other type of recognition of its own certificates otherwise mentioned above. No more guarantees can be pinpointed by the PMA and relying parties in their contractual relationship (if there is any).

9.8 Limitations of Liability

OPENTRUST makes no claims with regard to the suitability or authenticity of certificates issued under this CP. Relying parties may only use these certificates at their own risk. The PMA assumes no liability what so ever in relation with the use of certificate or associated public/private key pairs for any use other than those described in the present CP/CPS.

RA is liable as regards the accuracy of all information contained in the Subscriber certificate and Subscriber enrollment used for Consent Protocol and for Consent protocol operation.

9.9 Indemnities

OPENTRUST makes no claims as to the suitability of certificates issued under this CP for any purpose whatsoever. Relying parties use these certificates at their own risk. OPENTRUST has no obligation to make any payments regarding costs associated with the malfunction or misuse of certificates issued under this CP.

9.10 Term and Termination

9.10.1 Term

This CP and subsequent versions shall be effective upon approval by the PMA.

9.10.2 Termination

In the event that the PKI services ceases to operate, a public announcement must be made by the PMA. Upon termination of service, the PMA will properly archive its records including certificates issued, CP, CPS and CRL according to section 5.8 above.

9.10.3 Effect of Termination and Survival

End of validity of the present CP stops all obligation and liability for the PMA.

Sub-CA cannot continue delivering electronic certificate referred to by the present CP.

9.11 Individual Notices and Communications with Participants

The PMA provides all participants with new version of CP via the PS, as soon as it is validated by the PMA.

9.12 Amendments

9.12.1 Procedure for Amendment

The PMA reviews CP and CPS at least yearly. Additional reviews may be enacted at any time at the discretion of the PMA. Spelling errors or typographical corrections which do not change the meaning of the CP are allowed without notification. Prior to approving any changes to this CP, PMA notifies PKI components.

If the PMA wishes to recommend amendments or corrections to the CP, such modifications shall be circulated to appropriate parties identified by PMA. The PMA collects, sums up and proposes CP modifications according to approval procedures.

9.12.2 Notification Mechanism and Period

The PMA notifies PKI components on its intention to modify CP/CPS no less than 2 months before entering in a modification process of CP/CPS and according to the scope of modification.

9.12.3 Circumstances under Which OID Must Be Changed

The present CP OIDs have to be changed if the PMA determines that a change in the CP modifies the level of trust provided by the CP requirements or CPS material.

9.13 Dispute Resolution Provisions

Provisions for resolving disputes between OPENTRUST, DocuSign and its Clients shall be set forth in the applicable contract between the parties.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of FRANCE, shall govern the enforceability, construction, interpretation, and validity of the CP, irrespective of contract or other choice of law provisions and without the requirement to establish a commercial nexus in the State of France.

This governing law provision applies only to the CP. Contract with Client incorporating the CP by reference may have their own governing law provisions, provided that this section 9.14 governs the enforceability, construction, interpretation, and validity of the terms of the CP separate and apart from the terms of such other agreements, subject to any limitations appearing in applicable law.

9.15 Compliance with Applicable Law

The CP is subject to applicable French and European laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information and topics related to privacy and signature.

Client, DocuSign and OPENTRUST agree to conform to applicable laws and regulations in their contract.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CP constitutes the entire understanding between the parties and supersedes all other terms, whether expressed or implied by law. No modification of this CP shall be of any force or effect unless in writing and signed by an authorized signatory. Failure to enforce any or all of these sections in a particular instance or instances shall not constitute a waiver thereof or preclude subsequent enforcement thereof. All provisions in this CP which by their nature extend beyond the term of the performance of the services such as without limitation those concerning confidential information and intellectual property rights shall survive such term until fulfilled and shall apply to any party's successors and assigns.

9.16.2 Assignment

Except where specified by other contracts, only the PMA may assign and delegate this CP to any party of its choice.

9.16.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in section 9.12.

9.16.4 Waiver of Rights and obligation

No waiver of any breach or default or any failure to exercise any right hereunder shall be construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in the CP are for convenience only and cannot be used in interpreting the CP.

9.16.5 Force Majeure

OPENTRUST shall not be liable for any failure or delay in its performance under the CP due to causes that are beyond its reasonable control, including, but not limited to, an act of God, act of civil or military authority, natural disasters, fire, epidemic, flood, earthquake, riot, war, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action or any unforeseeable events or situations.

OPENTRUST HAS NO LIABILITY FOR ANY DELAYS, NON-DELIVERIES, NON-PAYMENTS, MIS-DELIVERIES OR SERVICE INTERRUPTIONS CAUSED BY ANY THIRD PARTY (like RA or Client) ACTS OR THE INTERNET INFRASTRUCTURE OR ANY NETWORK EXTERNAL TO OPENTRUST.

9.17 Other Provisions

9.17.1 Interpretation

All references in this CP to “sections” refer to the sections of this CP. As used in this CP, neutral pronouns and any variations thereof shall be deemed to include the feminine and masculine, and all terms used in the singular shall be deemed to include the plural, and vice versa as the context may require. The words “hereof,” “herein” and “hereunder” and other words of similar import refer to this CP as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this CP. The words "include" and “including” when used herein are not intended to be exclusive and mean, respectively, "include, without limitation" and “including, without limitation.”

9.17.2 Conflict of Provisions

In the event of a conflict between the provisions of this CP, the CPS and any subscriber agreement, the order of precedence shall be CP, CPS, and then subscriber agreement.

9.17.3 Limitation Period on Actions

Any legal actions involving a dispute that is related to this PKI or any services provided involving a certificate issued by this PKI shall be commenced prior to the end of date defined in contract between OPENTRUST, DocuSign and Client the period in dedicated by PMA after either the expiration of the certificate in dispute, or the date of provision of the disputed service or services involving the PKI certificate, whichever is earlier If any action involving a dispute related to a certificate issued by this PKI or any service involving certificates issued by this PKI certificate is not commenced prior to such time, any such action shall be barred.

9.17.4 Notice of Limited Liability

This CP makes no claims that should be construed to be an agreement between any parties, nor does it imply any liability for any parties.

10 CERTIFICATE AND CRL PROFILE

10.1 Sub-CA

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	C = FR O = OPENTRUST OU = OPENTRUST for Adobe CN = OPENTRUST CDS CA		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	2018/10/11 07:00:0 Z (Date of end of life of Issuer CA)		
Subject	**Attribute type**	**Attribute value**	**Directory String1**
	C	FR	PrintableString
	O	KEYNECTIS	PrintableString
	OU	KEYNECTIS for Adobe	PrintableString
	CN	KEYNECTIS K.Websign CDS	PrintableString
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	Sha1WithRSAEncryption (1.2.840.113549.1.1.5)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		9f 22 78 d7 71 1b de 33 b0 7f c9 20 7a a9 a8 e0 4e 62 e3 fb
Subject Key Identifier	**FALSE**	
Methods of generating key ID		ae 17 c5 29 d1 d9 51 e5 f9 04 d2 68 5a 28 92 e7 8f df 67 d7
Key Usage	**TRUE**	
keyCertSign		Set
cRLSign		Set
Extended Key Usage	**FALSE**	
Documents Acrobat authentiques 1.2.840.113583.1.1.5		Set
Certificate Policies	**FALSE**	
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.keynectis.com/PC/
policyQualifier-unotice		This certificate has been issued in accordance with the Acrobat Credentials CPS
Basic Constraint	**TRUE**	
cA		True

[1] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
pathLenConstraint		0
CRL Distribution Points	**FALSE**	
distributionPoint		http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_CDS_CA.crl
Reasons		n/a
cRLIssuer		n/a

10.2 Subscriber

Base Certificate	Value		
Version	2 (=version 3)		
Serial number	Defined by the software		
Issuer	CN = KEYNECTIS K.Websign CDS OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR		
NotBefore	YYYY/MM/DD HH:MM:SS Z (certificate issuance date)		
NotAfter	YYYY/MM/DD HH:MM:SS Z plus 5 minutes.		
Subject	**Attribute type**	**Attribute value**	**Directory String2**
	C	FR	PrintableString
	OU	RA *<Client name>*	UTF8String
	OU	*<Transaction identification number>*	UTF8String
	OU (optional)	*<filled according Client requirements>*	UTF8String
	OU (optional)	*<filled according Client requirements>*	UTF8String
	OU (optional)	*<filled according Client requirements>*	UTF8String
	CN	*<First name and Last name of Subscriber>*	UTF8String
Subject Public Key Info	Key generation (algorithm & OID)	rsaEncryption (1.2.840.113549.1.1.1)	
	Key size	2048	
Signature (algorithm & OID)	sha256WithRSAEncryption (1.2.840.113549.1.1.11)		

Extensions	Criticality (True/False)	Value
Authority Key Identifier	**FALSE**	
keyIdentifier		**ae 17 c5 29 d1 d9 51 e5 f9 04 d2 68 5a 28 92 e7 8f df 67 d7**
Subject Key Identifier	**FALSE**	
Methods of generating key ID		Defined by Software (SHA1 160bits of the subject public key)

[2] DirectoryString = TeletexString, PrintableString, UniversalString, UTF8String ou BMPString

Extensions	Criticality (True/False)	Value
Key Usage	**TRUE**	
Digital Signature		Set
Extended Key Usage	**FALSE**	
Documents Acrobat authentiques		1.2.840.113583.1.1.5
Certificate Policies	**FALSE**	
policyIdentifier		1.3.6.1.4.1.22234.2.8.3.12
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		This certificate has been issued in accordance with the Adobe CPS, OpenTrust Certificate Policy and OpenTrust PSGP 1.3.6.1.4.1.22234.2.4.6.1.9
policyIdentifier		1.2.840.113583.1.2.1
policyQualifier-cps		http://www.opentrust.com/PC/
policyQualifier-unotice		This certificate has been issued also in accordance with the Adobe CPS.
Basic Constraint	**TRUE**	
cA		False
pathLenConstraint		N/A
CRL Distribution Points	**FALSE**	
distributionPoint		http://trustcenter-crl.certificat2.com/Keynectis/KEYNECTIS_KWebsign_CDS.
Reasons		n/a
cRLIssuer		n/a
Authority Information Access	**FALSE**	
Ocsp		http://ocsp.certificat.com/keynectis-kwebsign-cds
Subject Alternative Name	**FALSE**	
rfc822Name		<Subscriber email address if transmitted to RA by Client>
Time stamping	**FALSE**	http://tsp.certificat.com/tsa-cds

10.3 CRL profile

CRL Fields	Value
Version	V2
Issuer DN	CN = KEYNECTIS K.Websign CDS OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR
ThisUpdate	Date of generation by CA
NextUpdate	Date of generation by CA + 7 days
Signature (algorithm & OID)	Sha256WithRSAEncryption (1.2.840.113549.1.1.11)

CRL Extension	Include	Critical (True/False)	Value
CRLNumber	Yes	False	Integer incremented

AKI	Yes	False	Issuer key hash
CRL Entry Fields	**Value**		
Revoked certificate serialNumber	Certificate Serial Number		
CRL Entry Extension	**Include**	**Critical (True/False)**	**Value**
Revocation Reason	Optional	False	[Should be revoked with unspecified reason]